

Manuel d'utilisation

v11.0

Serveur de messagerie MDaemon
Manuel d'utilisation

v11.0.0 - March 2010

Table des matières



Section I

1 Serveur de messagerie MDaemon 11.0

1.1 Introduction



Introduction

Développé par Alt-N Technologies, MDaemon est un serveur de messagerie basé sur les standards SMTP/POP3/IMAP fonctionnant sous Windows Vista/XP/2008/2003/2000 et offrant un grand nombre de fonctionnalités. MDaemon intègre des outils efficaces pour la gestion des comptes (dont le support d'Active Directory et LDAP), un serveur webmail, un filtre de contenu, des filtres anti-spam, des paramètres avancés de sécurité et bien plus encore.

MDaemon Standard, PRO et FREE

MDaemon est disponible en 3 versions : MDaemon Standard, PRO et FREE. MDaemon Standard inclut entre autres un serveur SMTP complet pour les entreprises souhaitant héberger elles-mêmes leur serveur de courrier, le support DomainPOP pour collecter le courrier chez un FAI, des listes de diffusion, le serveur webmail WorldClient...

MDaemon PRO contient toutes les fonctionnalités de MDaemon Standard, et ajoute : le support du protocole IMAP4, le support de plusieurs domaines, le partage de domaines, un système de passerelles, l'intégration avec les smartphones BlackBerry et de nombreuses autres fonctionnalités. Cette version convient donc aux entreprises nécessitant une solution plus complète. Avec MDaemon PRO, le serveur webmail s'agrémente également d'outils de travail collaboratif, d'une messagerie instantanée, d'un outil de création automatique de passerelles...

MDaemon FREE est une version limitée mais entièrement gratuite de MDaemon fournissant des fonctionnalités de base et acceptant jusqu'à 5 utilisateurs. MDaemon FREE supporte les protocoles SMTP et POP3 ainsi que l'administration à distance, et

inclut le webmail WorldClient, et diverses fonctionnalités. Pour en savoir plus sur les différences entre chaque version, consultez : www.altn.com.

Fonctionnalités de MDaemon

MDaemon ne se limite pas au traitement des e-mails. Voici un aperçu de ses fonctionnalités :

- Protection et analyse antivirus complète avec le module SecurityPlus for MDaemon. Les messages sont analysés et peuvent être nettoyés ou refusés automatiquement avant même d'être remis à leurs destinataires. SecurityPlus for MDaemon est un module additionnel vendu séparément.
- Listes de diffusion illimitées pouvant contenir des membres locaux ou externes, être publiques ou privées et proposant de nombreuses options...
- Serveur webmail WorldClient intégré. Il permet aux utilisateurs d'accéder à leur messagerie où qu'ils soient, à l'aide d'un simple navigateur.
- WorldClient permet également de programmer des rendez-vous et partager des dossiers, calendriers et tâches avec les autres utilisateurs. Il intègre un utilitaire de messagerie instantanée appelé ComAgent offrant un accès à la boîte de réception et aux dossiers de courrier sans ouvrir le navigateur.
- Sécurité : le filtre anti-spam et les listes noires DNS bloquent efficacement les spams. l'Écran IP et l'Écran d'hôte évitent que des adresses spécifiques envoient des messages à votre domaine ou utilisent votre système.
- Support du protocole LDAP (Lightweight Directory Access Protocol), des bases ODBC et de Active Directory pour la gestion des comptes. Plusieurs installations de MDaemon peuvent partager la même base de données des comptes.
- Il est possible de fournir une messagerie à tout un réseau local avec une simple boîte POP3 chez un FAI.
- MDaemon peut maintenir à jour le carnet d'adresses Windows ou Microsoft Outlook, ce qui constitue un moyen supplémentaire de fournir un carnet d'adresses global aux utilisateurs.
- Alias d'adresses permettant aux utilisateurs de posséder plusieurs adresses e-mail sur un ou plusieurs domaines.
- Passerelles : cet outil permet à MDaemon d'héberger temporairement le courrier de serveurs tiers avant de le transmettre au serveur distant (afin de le sécuriser ou de jouer le rôle de MX secondaire).
- Administration par le web avec le module intégré WebAdmin. Les administrateurs peuvent ainsi configurer le serveur MDaemon par le web et des droits d'accès spécifiques peuvent être attribués à chaque utilisateur afin de modifier les paramètres de leur compte.
- Avec les catalogues, l'administrateur peut mettre des fichiers à disposition des utilisateurs. Il suffit d'envoyer un message spécifique pour recevoir automatiquement le fichier demandé.
- Un système interne d’acheminement du courrier appelé messagerie RAW insère des messages dans le flux de courrier et simplifie considérablement le développement de modules personnalisés. Á l’aide de ce système, il est possible

de concevoir un système de messagerie électronique complet en utilisant un simple éditeur de texte et quelques fichiers batch.

- Filtre de contenu très flexible : automatise le traitement des messages en fonction de leur contenu (insertion/suppression d'en-têtes, ajout de pieds de page, suppression de pièces jointes, exécution de programmes...).

Configuration requise

Pour connaître le matériel requis et les systèmes supportés, consultez le site www.altn.com.

Voir également :

Nouveautés de MDaemon 11.0 14
Mise à jour vers MDaemon 11.0 16
Interface principale de MDaemon 22
Obtenir de l'aide 19

1.2 Nouveautés de MDaemon 11.0

Intégration avec BlackBerry Internet Service (BIS) (MDaemon PRO uniquement) 149

MDaemon supporte directement le service BlackBerry Internet Service (BIS). Les utilisateurs du service BIS de BlackBerry peuvent à présent intégrer leur compte MDaemon avec leur BlackBerry et bénéficier du push mail ainsi que d'une meilleure gestion du courrier lors de l'utilisation d'un BlackBerry avec MDaemon. Les BlackBerry configurés pour récupérer leur courrier de MDaemon via IMAP peuvent maintenant être configurés en push mail. De plus, le courrier rédigé sur les BlackBerry est distribué via MDaemon et non via les serveurs BIS. Ainsi, les messages envoyés depuis les BlackBerry sont soumis à la politique de sécurité de votre entreprise : Filtre de contenu, DKIM, archivage, etc.

BIS collecte uniquement le courrier se trouvant dans la boîte de réception, ce qui peut être génant pour les utilisateurs ayant créé des filtres IMAP 307 pour classer automatiquement les messages dans des dossiers spécifiques. Afin d'éviter ce problème, l'onglet Courrier BlackBerry 325 de l'Éditeur de compte et la page Dossiers de WorldClient permettent respectivement aux administrateurs et aux utilisateurs de choisir les dossiers à synchroniser. Lorsque le service BIS se connecte à MDaemon pour collecter le courrier, MDaemon envoie le contenu des dossiers sélectionnés. Tous les messages provenant des dossiers sélectionnés sont envoyés dans le dossier Messages du BlackBerry. Ces messages restent dans leurs dossiers respectifs sur le serveur MDaemon et les dossiers ne sont pas créés sur le BlackBerry. Ils sont simplement envoyés sur le BlackBerry comme s'ils appartenaient au dossier de courrier.

Enfin, un système d'alias interne lie les dossiers Éléments envoyés et Éléments supprimés (quels que soient leurs noms) à des valeurs reconnues par BIS. Cela permet de s'assurer que les messages envoyés et supprimés soient placés dans les dossiers

correspondants de MDaemon.

Optimisation du routage des messages 34

Une nouvelle option (activée par défaut) a été ajoutée à l'onglet Distribution 34 des paramètres du domaine par défaut. Avec cette option, MDaemon conserve une seule copie des messages ayant plusieurs destinataires et utilise ensuite des commandes RCPT pour distribuer le message. Cela permet d'économiser de l'espace disque et de la bande passante. Cette option est utile si par exemple un même message est destiné à plusieurs utilisateurs du domaine. De plus, si vous utilisez l'option de distribution envoyant tout le courrier sortant à une IP/un domaine/un hôte spécifique, MDaemon conserve une seule copie de chaque message et utilise plusieurs commandes RCPT même lorsque les destinataires appartiennent à des domaines différents.

Amélioration du support des clients SyncML 122

Ajout du support de la version 8.0 des clients SyncML open source Funambol. Ces clients sont disponibles gratuitement et ont été considérablement améliorés par rapport aux versions précédentes, en particulier en ce qui concerne le client pour BlackBerry.

Liens vers les pièces jointes (MDaemon PRO uniquement) 139

Cette fonctionnalité retire les pièces jointes des messages et les stocke sur le serveur MDaemon. Lorsqu'un utilisateur ouvre un message, celui-ci contient des liens sur lesquels il peut cliquer pour récupérer les pièces jointes. Cela permet d'économiser de la bande passante et de l'espace de stockage, en particulier sur les appareils mobiles. Dans MDaemon 11.0, cette fonctionnalité a été entièrement retravaillée afin de la rendre plus intuitive et plus simple d'utilisation. Les options ne se trouvent plus dans les paramètres des comptes, mais dans "Configuration » Web, Synchro, & MI," car WorldClient joue un rôle important. Deux modes sont à présent disponibles : "*Laisser WorldClient configurer automatiquement les liens vers les pièces jointes*" et "*Configurer manuellement les liens vers les pièces jointes*". En mode automatique (option par défaut) cet outil fonctionne avec des paramètres internes que les utilisateurs ne peuvent pas modifier. Il s'agit de la solution la plus simple : aucune configuration n'est nécessaire, il suffit simplement que WorldClient soit démarré. Le mode manuel permet de choisir l'emplacement auquel sont stockées les pièces jointes.

Les modifications suivantes ont également été apportées au système de liens vers les pièces jointes :

- Les pièces jointes de tous les comptes configurés pour utiliser cet outil dans une version précédente seront extraites dans le répertoire FILES. Vous devrez donc peut-être reconfigurer manuellement les comptes utilisant les liens vers les pièces jointes.
- Si vous désactivez cette fonctionnalité, les paramètres des comptes sont conservés. Ainsi, si vous l'activez à nouveau ultérieurement, il ne sera pas nécessaire de reconfigurer les comptes.
- Les URL placées dans les messages ne contiennent plus des chemins complets. Un identifiant unique (GUID) est généré et utilisé pour lier une URL à un fichier sur le disque. Les liens des GUID sont stockés dans le fichier `AttachmentLinking.dat`.

- Le modèle de compte 330 a également été mis à jour afin de pouvoir déterminer la gestion des pièces jointes pour les nouveaux comptes.

DKIM ADSP - support de la RFC 5617 258

DKIM ADSP (Author Domain Signing Practices) a été finalisé et rendu public dans la RFC 5617. DKIM (DomainKeys Identified Mail) est un système d'authentification au niveau du domaine permettant de vérifier la source et le contenu des messages. ADSP est un outil complémentaire permettant d'évaluer les messages qui ne contiennent pas de signature DKIM pour le domaine indiqué dans l'adresse de l'expéditeur (en-tête FROM:). L'enregistrement ADSP indique si le domaine signe son courrier sortant ainsi que la façon dont les autres hôtes peuvent accéder à cet enregistrement.

MDaemon a été mis à jour afin de supporter la version finale de cette spécification. Aucune modification n'est requise pour les enregistrements DKIM ou ADSP existants. Cela représente l'aboutissement de plus de 4 ans d'efforts à l'IETF. Alt-N recommande fortement l'utilisation de ce protocole, avec lequel MDaemon est entièrement compatible. Il est également recommandé de publier votre propre enregistrement ADSP dans vos DNS afin d'informer les autres hôtes sur votre politique de signature. ADSP s'active dans l'onglet Options DKIM 258.

STLS pour DomainPOP et MultiPOP 272

Les serveurs DomainPOP et MultiPOP de MDaemon supportent STLS. L'option permettant de l'activer se trouve dans : Sécurité » Paramètres de sécurité » SSL & TLS » MDaemon. Lorsque cette option est activée la connexion est tentée avec STLS, mais si l'autre partie ne supporte pas cette commande, une connexion normale est établie. Le fichier `NoSTARTTLS.DAT` contient la liste des sites auxquels cette option ne s'applique pas.

Modifications et nouvelles fonctionnalités

Pour obtenir une liste complète des nouvelles fonctionnalités et modifications apportées à MDaemon 11.0, consultez le fichier `RelNotes.html` situé dans le sous-dossier `\Docs\` du répertoire d'installation de MDaemon.

Voir également :

Introduction 12
Mise à jour vers MDaemon 11.0 16
Interface principale de MDaemon 22

1.3 Mise à jour vers MDaemon 11.0

Vous trouverez ci-dessous un ensemble de remarques et de considérations spéciales à prendre en compte lors du passage de votre ancienne version à la version 11.0 de MDaemon.

Version 11.0.0

- La connexion aux serveurs POP et IMAP de MDaemon requiert à présent l'adresse e-mail complète. Si le client de messagerie d'un utilisateur est configuré pour utiliser uniquement la boîte aux lettres il ne pourra pas se connecter. Les clients POP/IMAP doivent être modifiés de façon à utiliser l'adresse e-mail complète en tant qu'identifiant. Si vous souhaitez continuer à autoriser les connexions utilisant uniquement le nom de la boîte aux lettres, désactivez l'option "*Exiger l'adresse e-mail complète pour l'authentification sur les serveurs*", dans l'onglet Système159 des Préférences (ceci est fortement déconseillé).

- Le système de liens vers les pièces jointes139 a été entièrement modifié et les paramètres ont du être rétablis à leurs valeurs par défaut. Lors de la mise à jour vers MDaemon 11.0, les pièces jointes de tous les comptes configurés pour utiliser cet outil dans une version précédente seront extraites dans le répertoire FILES. Vous devrez donc peut-être reconfigurer manuellement les comptes utilisant les liens vers les pièces jointes.

- `WorldClient.dll` a été mis à jour pour générer dynamiquement le fichier `robots.txt` file dans le répertoire HTML de WorldClient afin d'indiquer quels fichiers ne doivent pas être indexés, sauf si `WorldClient.ini` est configuré comme suit :
  `[WebServer]`
  `ModifyRobotsTxt=No`.
  Si le fichier `robots.txt` est en lecture seule il ne sera pas modifié. La balise meta suivante doit être insérée dans l'en-tête des fichiers Logon.html personnalisés : `<meta name="ROBOTS" content="NOINDEX, FOLLOW">`.

- Les thèmes Globe et Redline ont été supprimés de WorldClient et ne sont plus supportés. Lorsque MDaemon 11 est exécuté pour la première fois, les dossiers \Templates\ et \HTML\ de ces deux thèmes sont déplacés dans \WorldClient\Old\. Ces dossiers peuvent être supprimés en toute sécurité, sauf si vous décidez de maintenir ces thèmes manuellement.

- *Check a DKIM DNS Record* (http://dkimcore.org/tools/dkimrecordcheck.html) est un outil permettant de vérifier si vos paramètres DNS DKIM sont conformes à la spécification DKIM publiée dans la RFC 4871. En indiquant le sélecteur et le nom de domaine, cet outil repère l'enregistrement DKIM dans les DNS, l'analyse avec le BNF de la spécification DKIM, puis vérifie la validité du contenu. Le résultat obtenu vous indique si votre configuration DNS DKIM est conforme à la spécification. Remarque : ce site est encore en cours de création et n'est ni hébergé ni créé par Alt-N Technologies.

- Les options du calcul des quotas ont été réinitialisées à leurs valeurs par défaut. Consultez les paramètres de l'onglet Quotas367 pour les vérifier ou les rétablir. L'option "*Inclure tous les sous-dossiers de la boîte de réception dans le calcul des quotas*" est à présent activée par défaut.

- Dans le cadre de l'intégration avec BlackBerry Internet Service (BIS)149, MDaemon requiert que toutes les sessions IMAP/POP d'utilisateurs de BlackBerry utilisent leur adresse e-mail complète en tant que nom d'utilisateur pour la collecte IMAP et/ou POP. Ainsi, lors de la création du profil de messagerie sur le BlackBerry, les utilisateurs devront indiquer l'adresse e-mail complète pour le nom d'utilisateur. Cela est nécessaire pour éviter d'éventuels conflits et intégrer

correctement les comptes. Certains utilisateurs ayant déjà créé un profil de messagerie devront le supprimer et le recréer ou modifier leur nom d'utilisateur.

Version 10.1.0

- Suite aux nombreuses améliorations apportées au thème LookOut dans les dernières versions de MDaemon ainsi qu'aux progrès des technologies et standards du web depuis 2001, le thème LookOut ne supporte plus Internet Explorer 6. Les utilisateurs d'une version 6 ou inférieure de Internet Explorer seront redirigés vers le thème Standard afin de pouvoir accéder à leur messagerie. Il est toutefois recommandé pour les utilisateurs d'effectuer une mise à jour vers Internet Explorer 8 qui apporte d'importantes améliorations en termes de sécurité, qualité d'affichage et performance.

Version 10.0.3

- Le code de la fonctionnalité DNS-BL 231 a été modifié. Il est possible que cette fonctionnalité soit désactivée après l'installation de la mise à jour. Vous pouvez l'activer simplement dans : Sécurité » Filtre anti-spam... » DNS-BL.

Remarques spécifiques à la version 10.0.0

- Cette version **N'EST PAS** compatible avec les versions précédentes. Lorsqu'elle est installée pour la première fois, des modifications irréversibles sont effectuées dans les fichiers de configuration. **Pensez à effectuer une sauvegarde avant d'installer cette version.**
- Les fichiers de configuration pour la collecte du courrier 141 et les mises à jour antivirus 147 et anti-spam 227 ont été modifiés. Par conséquent, toutes ces programmations seront rétablies aux valeurs par défaut. Veuillez vérifier ces options et rétablir les programmations de votre choix.
- Le fichier d'index des messages de WorldClient a changé. La première connexion d'un utilisateur risque d'être lente, car il sera mis à jour au nouveau format. Les connexions suivantes se feront à vitesse normale.
- Les paramètres DNS-BL 231 ont été réinitialisés. Pensez à la vérifier et à rétablir la configuration. Ces paramètres se trouvent dans la nouvelle interface du Filtre anti-spam.
- La version Standard de MDaemon ne supporte plus les Passerelles 406. Si vous souhaitez bénéficier de cette fonctionnalité, vous devez posséder MDaemon PRO.
- MDaemon Standard est à présent limité à 5 listes de diffusion avec un maximum de 50 membres chacune. Si vous souhaitez utiliser plus de listes ou pouvoir inscrire plus de membres, vous devez posséder MDaemon PRO.
- L'option "Toujours afficher les données enregistrées" dans Journalisation » Options 98 a été rétablie à sa valeur par défaut (désactivée). N'oubliez pas de la réactiver si nécessaire.
- Le fichier Signature.dat n'est plus utilisé. Les signatures des comptes individuels sont à présent stockées dans des fichiers <email>.sig se trouvant dans le nouveau dossier Signatures. Lors de l'installation, MDaemon lit le fichier

Signature.dat et transfère les signatures existantes dans les nouveaux fichiers. Si vous utilisez une signature de domaine par défaut, vous devrez la redéfinir.

- Pour obtenir une liste complète des nouvelles fonctionnalités et modifications apportées à cette version de MDaemon, consultez le fichier Relnotes.txt situé dans le sous-dossier \Docs\ de MDaemon.

Voir également :

Introduction 12
Nouveautés de MDaemon 11.0 14
Interface principale de MDaemon 22

1.4 Obtenir de l'aide

Options de support

Le support fait partie intégrante de l'expérience utilisateur chez Alt-N Technologies. Nous souhaitons vous faire bénéficier au mieux de nos produits longtemps après l'achat et l'installation initiale, et nos équipes se dédient à la résolution de vos problèmes afin de vous apporter une entière satisfaction. Pour en savoir plus sur le service client, les possibilités de support technique, les ressources techniques, les informations produits, etc., consultez la page de support d'Alt-N Technologies à l'adresse : www.altn.com/support/

Test des versions bêta de MDaemon

Alt-N Technologies offre à ses utilisateurs la possibilité de participer au test des versions bêta. Si vous souhaitez des informations sur la communauté de bêta testeurs, il suffit d'envoyer un e-mail à l'adresse : MDaemonBeta@altn.com.



Les versions bêta sont destinées aux personnes souhaitant participer aux tests des nouvelles versions avant leur sortie. Il ne s'agit en aucune façon d'un outil de support technique. Le support technique est uniquement disponible via les méthodes indiquées à l'adresse www.altn.com/support/.

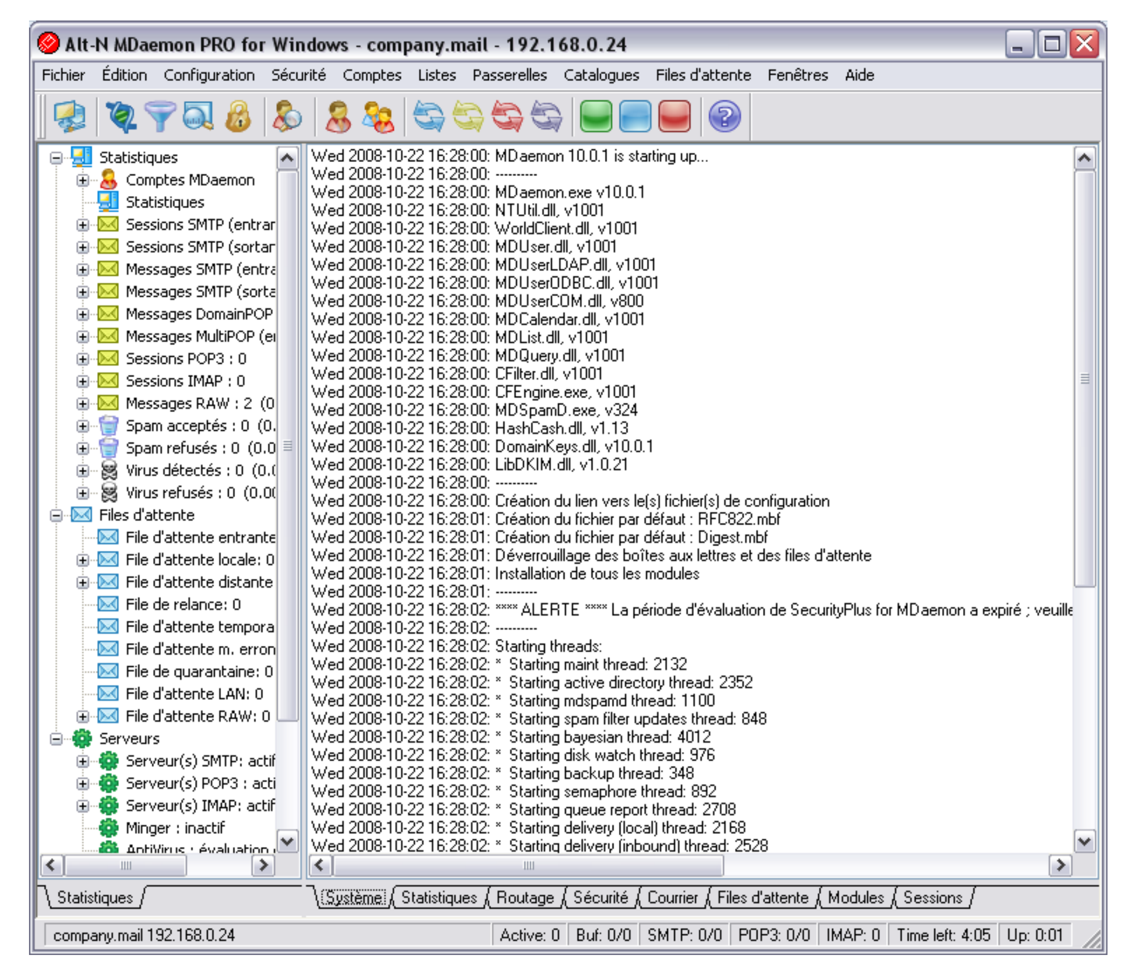
Contact

Alt-N Technologies, Ltd.
2550 SW Grapevine Parkway, Suite 150
Grapevine, Texas 76051
Tél. gratuit pour les États-Unis : 866-601-ALTN (2586)
Tél. pour l'international : 817-601-3222
Fax : 817-601-3223



Section II

2 Interface principale de MDaemon



Cette fenêtre fournit des informations importantes sur les ressources, les statistiques, les sessions actives et le courrier en attente de traitement. Elle contient également des options pour activer et désactiver facilement les différents serveurs de MDaemon. Ses différents onglets indiquent l'activité du serveur et des connexions entrantes et sortantes.

Statistiques

Situé à gauche de l'écran, ce panneau comporte trois sections : Statistiques, Files d'attente et Serveurs.

La section Statistiques contient les statistiques relatives au nombre de messages envoyés et reçus par MDaemon, ainsi que le nombre de sessions POP3 et IMAP initialisées depuis le démarrage de l'application. Cette section indique également le nombre de comptes utilisateurs existants, et le nombre de comptes pouvant encore être créés.



Lorsque l'on clique sur Remettre la racine des compteurs à zéro, cela concerne tous les compteurs et pas uniquement le compteur sélectionné. De plus il existe une option appelée *Conserver les valeurs des racines des compteurs de messages au redémarrage* dans Configuration » Préférences » GUI. Si elle n'est pas activée, ces valeurs sont remises à zéro à chaque redémarrage du serveur.

La section Files d'attente contient une entrée pour chaque message en attente et présente le nombre de messages (s'il y en a) dans chaque file. En effectuant un clic droit sur l'un des messages de la file, vous avez accès à une ou plusieurs des options suivantes en fonction de la file sélectionnée :

Afficher la file—cette option affiche l'onglet Files d'attente et la file sélectionnée directement dans l'interface principale. Il contient une liste de tous les messages de la file. De nombreuses options similaires à celles du Gestionnaire de files d'attente et de statistiques sont disponibles en effectuant un clic droit sur un message (Copier, Déplacer, Modifier, Liste blanche) etc.

Gestionnaire de files d'attente et de statistiques—ouvre le Gestionnaire de files d'attente et de statistiques avec la file sélectionnée.

Traiter maintenant—remet tout les messages en file d'attente et essaie de les distribuer normalement. Si vous effectuez cette action pour les messages de la File d'attente temporaire ou ceux de la File d'attente des messages erronés, ils risquent de générer les mêmes erreurs et d'être renvoyés dans ces listes.

Figer/ne pas figer la file d'attente—arrête temporairement le traitement d'une liste sélectionnée, ou le reprend s'il était en pause.

Distribuer—distribue les messages de la File d'attente temporaire, sans tenir compte des erreurs rencontrées : même si ces erreurs se reproduisent, les messages ne seront pas renvoyés cette file.

Remettre en file d'attente—cette option s'applique à la File temporaire et fonctionne de façon identique à l'option *Traiter maintenant* ci-dessus.

Activer / désactiver la file d'attente—active ou désactive la File temporaire. Lorsque cette option est désactivée, les messages ne sont pas déplacés dans cette file, même si des erreurs se produisent.

La section Serveurs contient une entrée pour chaque serveur de MDaemon, qui indique son état ("Actif" ou "Inactif"). Si un serveur est actif, vous trouverez sous l'entrée correspondante le port et l'adresse IP qu'il utilise. Vous pouvez effectuer un clic droit sur un serveur pour modifier son état. Lorsqu'un serveur est inactif, son icône est rouge.

Suivi des événements et journalisation

Le volet de droite de l'interface principale contient plusieurs onglets. Ils affichent l'état des différents serveurs et ressources de MDaemon, et sont actualisés fréquemment pour rendre compte de l'état du serveur. L'activité de chaque session SMTP/POP/IMAP et des autres serveurs est enregistrée dans l'onglet approprié lorsqu'une session est terminée, afin qu'un enregistrement de l'activité du réseau soit toujours disponible. Les

informations affichées dans ces onglets sont également inscrites dans les fichiers journaux se trouvant dans le répertoire Logs si vous avez choisi d'enregistrer l'activité des serveurs.

Le volet principal de l'interface MDaemon contient les onglets suivants :

Système—Au démarrage du programme, l'onglet Système affiche un enregistrement du processus d'initialisation, qui peut vous signaler d'éventuels problèmes de configuration ou d'état de MDaemon. Il affiche également l'activité, comme par exemple l'activation ou la désactivation d'un des différents serveurs de MDaemon.

Statistiques—Affiche le rapport de statistiques du serveur. Il contient les mêmes valeurs que l'onglet Statistiques. Il est possible d'en personnaliser la police en modifiant le fichier MDaemon.ini :

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

De plus, le postmaster ainsi que les destinataires des notifications 194 du Filtre de contenu reçoivent ce rapport tous les jours à minuit. Ce rapport est le même que celui généré lorsque la commande "Status" est envoyée au serveur par e-mail. Si vous souhaitez désactiver l'envoi, décochez la case "*Envoyer le résumé des statistiques au postmaster à minuit*" dans l'onglet Divers 167 des Préférences.

Routage—Affiche les informations de routage (destinataire, expéditeur, id du message, etc.) pour chaque message traité par MDaemon.

Sécurité

Filtre de contenu—Affiche les opérations du Filtre de contenu 178 de MDaemon. Lorsqu'un message répond aux critères établis par l'une des règles du Filtre, les informations importantes concernant le message et les actions entreprises sont enregistrées ici.

Antivirus—Si SecurityPlus for MDaemon 177 est installé, toutes les opérations de l'antivirus sont recensées dans cet onglet. Lorsqu'un message est analysé, les informations importantes le concernant et les actions entreprises sont enregistrées ici.

Anti-spam—Activités de prévention et de filtrage du spam 208.

MDSpamD—Activité du Daemon anti-spam 218.

SPF/Sender ID—Activité des systèmes Sender Policy Framework et Sender ID 249.

DK/DKIM—Activité des systèmes DomainKeys et DomainKeys Identified Mail 251.

Certification VBR—Activité du sytème de Certification VBR 260.

Analyse—Activité du système de répulsion 288 et de l'Ecran dynamique 269.

Courrier

SMTP (entrant)—Activité des sessions entrantes qui utilisent le protocole

SMTP.

SMTP (sortant)—Activité des sessions sortantes qui utilisent le protocole SMTP.

IMAP—Sessions de messagerie utilisant le protocole IMAP.

POP3—Lorsque des utilisateurs reçoivent du courrier depuis MDaemon à l'aide du protocole POP3, cette activité est enregistrée ici.

MultiPOP—Activité de collecte du courrier MultiPOP de MDaemon.

DomainPOP—Activité DomainPOP de MDaemon.

LDAP—Activité du serveur LDAP.

Minger—Activité du serveur Minger 369.

RAW—Activité des messages RAW, ou de ceux générés par le système.

Outlook Connector—Activité de Outlook Connector.

BIS — Activité de l'intégration avec BlackBerry Internet Service 151.

WorldClient—Activité des sessions WorldClient.

SyncML—Contient les données présentes dans le journal SyncML.

Files d'attente—Affiche des onglets pour chaque file d'attente : Locale, Distante, Temporaire, Quarantaine, Bayésien-spam, etc.

Modules—Activité des modules de MDaemon.

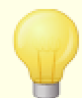
Sessions—D'autres onglets s'affichent en cliquant sur cet onglet. Chaque entrée correspond à une connexion active (SMTP/POP entrantes ou sortantes, IMAP, WorldClient...). Double cliquez sur une session 27 pour afficher le transcript.



Les informations affichées dans ces onglets n'ont pas d'incidence sur la quantité de données enregistrées dans les fichiers journaux. Toutefois, MDaemon est particulièrement flexible en ce qui concerne la quantité et le type d'informations enregistrées dans ces fichiers. Voir la page Journalisation 92 pour en savoir plus.

Menu contextuel

Un menu contextuel est disponible en effectuant un clic droit dans l'un des onglets du panneau de droite. Il permet de sélectionner, copier, supprimer ou enregistrer le contenu des onglets. L'option Imprimer/Copier affiche le texte sélectionné dans le Bloc-notes, afin de pouvoir l'imprimer ou enregistrer le fichier. L'option Rechercher affiche toutes les transcriptions de session contenant les termes recherchés compilées dans un fichier ouvert dans le Bloc-notes afin de faciliter la lecture.



L'affichage des volets dans l'interface principale de MDaemon n'est pas limité aux emplacements par défaut décrits ci-dessus. Vous pouvez modifier la mise en page en cliquant sur

le menu Fenêtres » Inverser les volets.

Affichage détaillé du journal

L'option Vue Journal détaillé se situe dans le menu Fenêtres de la barre des menus de MDaemon. En cliquant sur cette option, une fenêtre de l'interface principale s'ouvre ; elle rassemble les informations affichées dans un ou plusieurs onglets de l'interface. Vous pouvez modifier les éléments affichés dans cette fenêtre à l'aide des options se trouvant dans l'onglet Journal détaillé95 des options de journalisation du domaine principal.

Voir également :

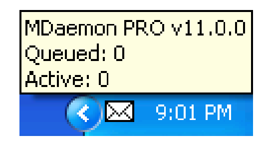
Fenêtre de session 27
Icône de la zone de notification 26
Menu contextuel 27

2.4 Icône de la zone de notification

Lorsque MDaemon fonctionne, cette icône figure dans la zone de notification. Elle permet non seulement de savoir si le serveur fonctionne, mais elle est également dynamique et change de couleur en fonction de l'état du serveur :

	Tout va bien. Pas de courrier dans les files d'attente locale ou distante.
	Tout va bien. Du courrier dans les files d'attente locale ou distante.
	Espace disque disponible inférieur au seuil indiqué (voir Configuration » Préférences » Disque161).
	Le réseau est hors service, la connexion a échoué ou le disque est plein.
L'icône clignote	Une nouvelle version de MDaemon est disponible.

Des informations complémentaires concernant le serveur sont disponibles dans l'info-bulle de l'icône. Pour cela, placez le curseur de la souris sur l'icône :



Menu contextuel

Ce menu s'affiche en effectuant un clic droit sur l'icône et permet d'accéder rapidement à la plupart des menus de MDaemon, sans devoir ouvrir l'interface.

Cliquez sur les options À propos de MDaemon/Alt-N … pour en savoir plus sur MDaemon ou Alt-N Technologies.

La troisème section contient les menus : Configuration, Sécurité, Comptes, Listes, Passerelles, Catalogues et Files d'attente. Chacun de ces menus en cascade est identique au menu du même nom qui se trouve dans la barre de menus de l'interface principale.

La quatrième section contrôle l'ouverture du gestionnaire de comptes, du gestionnaire de files et statistiques, et le traitement des files d'attente de courrier de MDaemon.

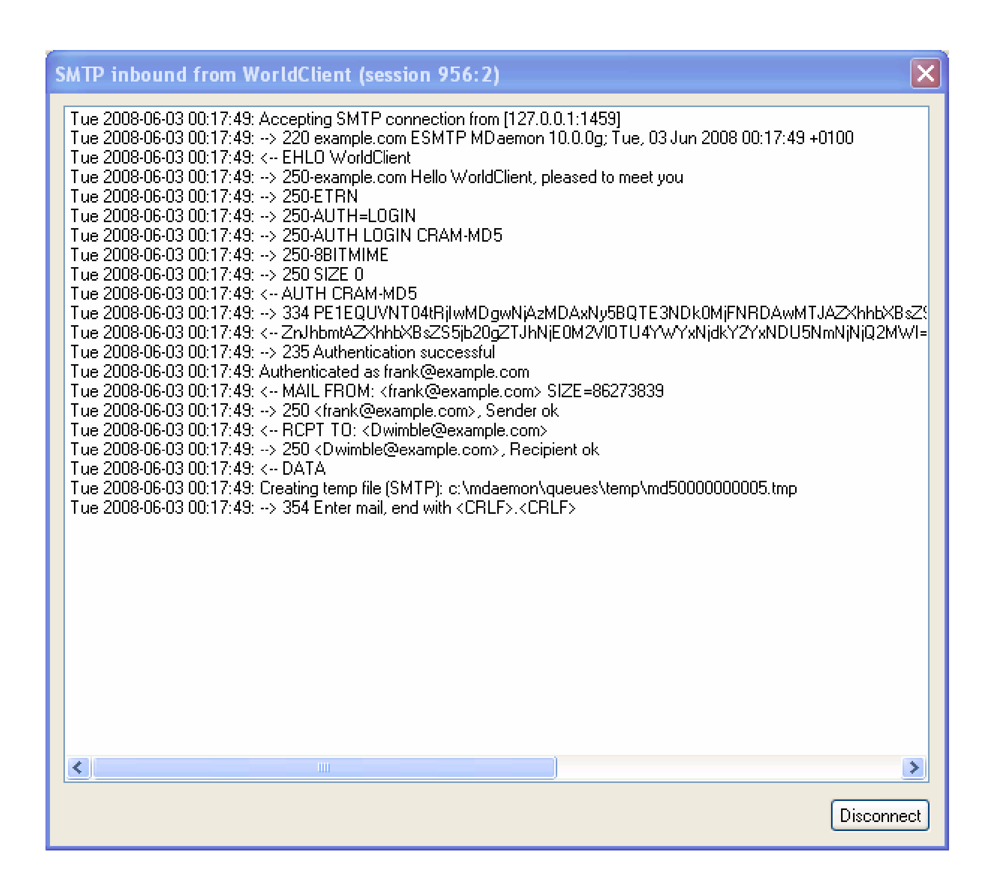
La dernière option "Arrêter MDaemon," ferme l'application ou arrête le service (les paramètres du service ne sont pas modifiés).

Verrouiller/déverouiller l'interface

Pour verrouiller l'interface utilisateur, réduisez la fenêtre de MDaemon, cliquez sur Verrouiller le serveur…, puis saisissez un mot de passe dans la boîte de dialogue qui s'ouvre. Une fois que vous avez confirmé le mot de passe en le saisissant une seconde fois, l'interface utilisateur de MDaemon est verrouillée ; elle ne peut pas être ouverte ni affichée, bien que MDaemon continue de fonctionner normalement. Toutefois, vous pouvez toujours utiliser l'option Traiter toutes les files maintenant… du menu, afin de traiter toutes les files d'attente de courrier manuellement si vous le souhaitez. Pour déverrouiller MDaemon, double-cliquez ou cliquez avec le bouton droit de la souris sur l'icône de la zone de notification. Sélectionnez ensuite Ouvrir MDaemon… ou Déverrouiller le serveur…, puis entrez le mot de passe que vous avez créé lors du verrouillage.

2.5 Fenêtre de session

Cette fenêtre s'affiche lorsque l'on double-clique sur une session active dans l'un des onglets Session 23 de l'interface principale. Elle indique en temps réel le transcript SMTP de la session en cours. Cliquez sur le bouton Déconnecter si vous souhaitez interrompre cette session.

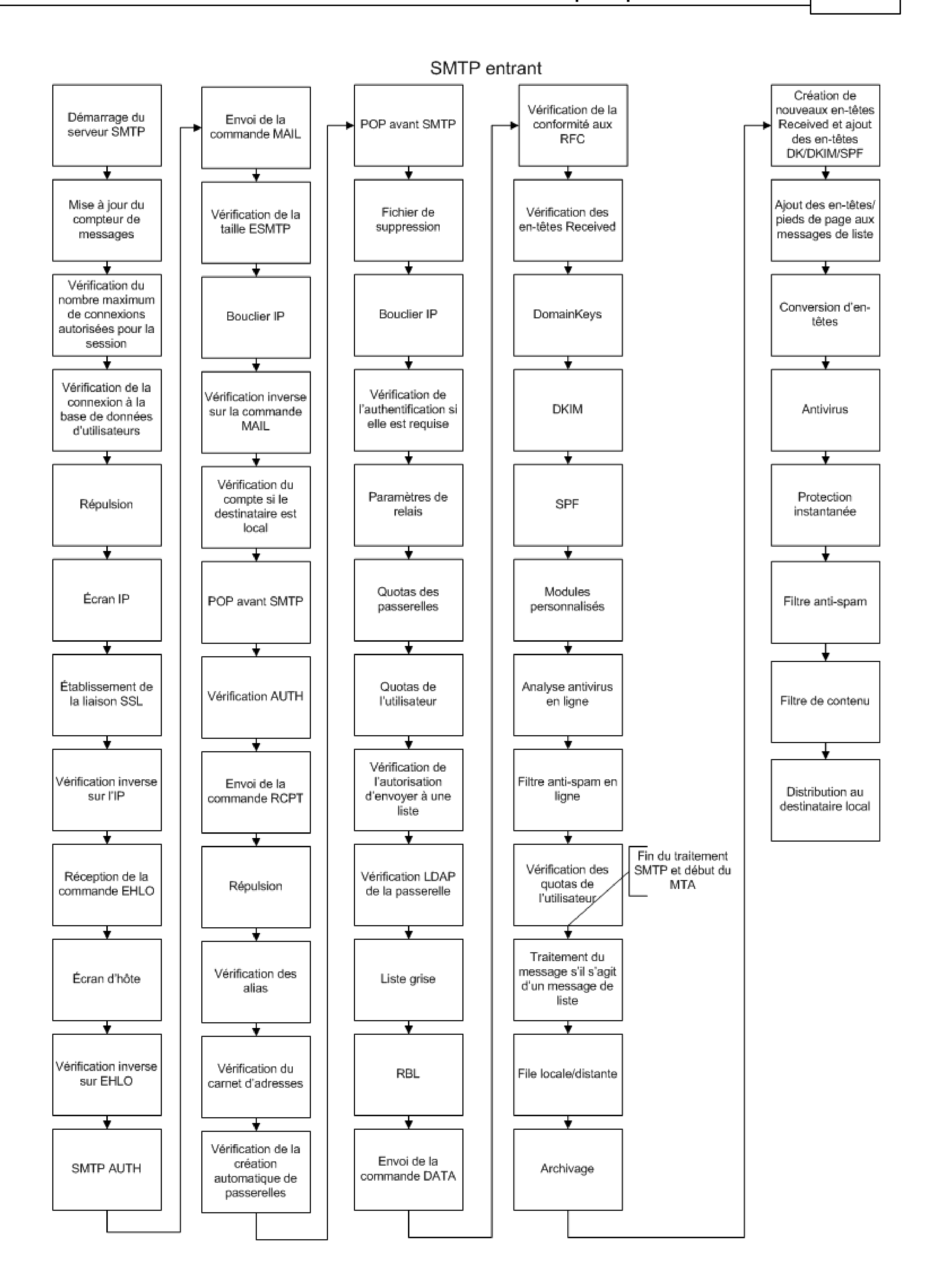


2.6 Flux SMTP de MDaemon

Lors d'une connexion SMTP entrante, MDaemon effectue une série complexe d'étapes de traitement visant à déterminer s'il faut accepter et distribuer le courrier, et quelles actions entreprendre après l'avoir accepté. Le graphique suivant représente ce flux pour les messages SMTP entrants.



Ces étapes peuvent être exécutées plus ou moins différemment en fonction de votre configuration. Une ou plusieurs d'entre elles peuvent être ignorées si une fonctionnalité donnée a été désactivée.


SMTP entrant
Démarrage du serveur SMTP
Mise à jour du compteur de messages
Vérification du nombre maximum de connexions autorisées pour la session
Vérification de la connexion à la base de données d'utilisateurs
Répulsion
Écran IP
Établissement de la liaison SSL
Vérification inverse sur l'IP
Réception de la commande EHLO
Écran d'hôte
Vérification inverse sur EHLO
SMTP AUTH
Envoi de la commande MAIL
Vérification de la taille ESMTP
Bouclier IP
Vérification inverse sur la commande MAIL
Vérification du compte si le destinataire est local
POP avant SMTP
Vérification AUTH
Envoi de la commande RCPT
Répulsion
Vérification des alias
Vérification du carnet d'adresses
Vérification de la création automatique de passerelles
POP avant SMTP
Fichier de suppression
Bouclier IP
Vérification de l'authentification si elle est requise
Paramètres de relais
Quotas des passerelles
Quotas de l'utilisateur
Vérification de l'autorisation d'envoyer à une liste
Vérification LDAP de la passerelle
Liste grise
RBL
Envoi de la commande DATA
Vérification de la conformité aux RFC
Vérification des en-têtes Received
DomainKeys
DKIM
SPF
Modules personnalisés
Analyse antivirus en ligne
Filtre anti-spam en ligne
Vérification des quotas de l'utilisateur
Fin du traitement SMTP et début du MTA
Traitement du message s'il s'agit d'un message de liste
File locale/distante
Archivage
Création de nouveaux en-têtes Received et ajout des en-têtes DK/DKIM/SPF
Ajout des en-têtes/ pieds de page aux messages de liste
Conversion d'en-têtes
Antivirus
Protection instantanée
Filtre anti-spam
Filtre de contenu
Distribution au destinataire local



Section III

3 Menu Configuration

3.1 Domaine/serveurs par défaut

3.1.1 Domaine & serveurs par défaut

Ces paramètres sont accessibles depuis le menu Configuration » Domaine/serveurs par défaut... Vous ne pouvez créer qu'un seul domaine par défaut, mais MDaemon peut également gérer un nombre illimité de Domaines supplémentaires103 (MDaemon PRO uniquement), et stocker le courrier de plusieurs Passerelles de domaine406.

La section Domaine & serveurs par défaut contient les onglets suivants :

Domaine33
Nom et adresse IP du domaine.

Distribution34
Vous avez le choix entre deux options : soit MDaemon distribue lui-même le courrier, soit il le relaie à un FAI, une passerelle ou un hôte spécifique qui distribueront le courrier à sa place.

Serveurs38
Options relatives aux serveurs et aux protocoles de courrier.

Ports41
Ports utilisés par MDaemon pour la distribution du courrier POP et SMTP ; ainsi que le port sur lequel MDaemon écoute les événements IMAP et le port UDP utilisé pour interroger les serveurs DNS. Dans la plupart des cas, les paramètres par défaut n'ont pas à être modifiés. Toutefois, il est utile de savoir configurer ces ports si vous souhaitez intégrer MDaemon avec d'autres applications sur votre système.

DNS43
Désigne les adresses IP du serveur DNS primaire et du serveur DNS secondaire. Cet onglet contient également différentes options de traitement des enregistrements MX.

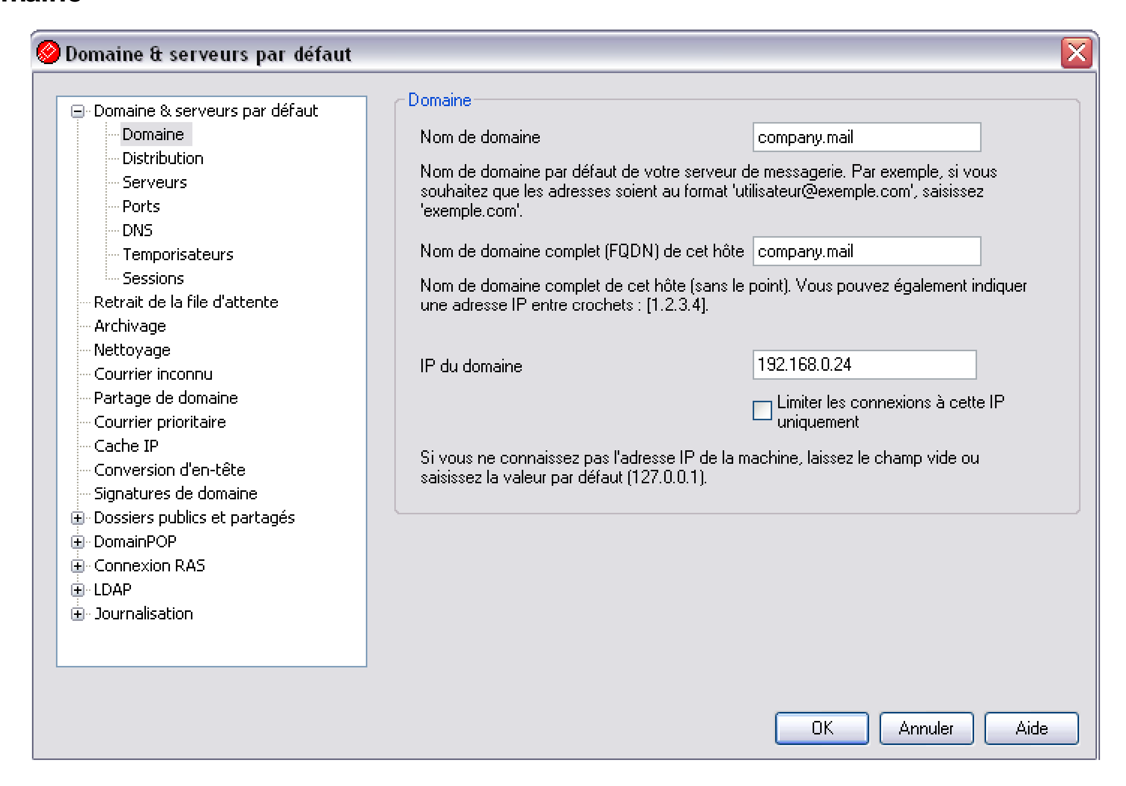
Temporisateurs47
Contient plusieurs limites de temps respectées par MDaemon lorsqu'il se connecte à des hôtes distants, attend l'échange de protocoles, la réponse des DNS, etc. De plus, cet onglet permet de fixer le nombre maximal de sauts de message, option destinée à empêcher que le courrier ne soit distribué en boucle.

Sessions47
Indiquez ici le nombre maximal de sessions simultanées que MDaemon peut ouvrir pour envoyer ou recevoir du courrier SMTP, POP et IMAP. Définissez également le nombre de messages que MDaemon essaie d'envoyer et de recevoir en même temps.

Voir également :

Hébergement de plusieurs domaines 101
Domaines supplémentaires 103
Passerelles 406
Collecte DomainPOP 72

3.1.1.1 Domaine



Domaine

Nom de domaine
Il s'agit du nom de domaine par défaut utilisé lors de la création de comptes. Il est également utilisé pour la création automatique de comptes dans WorldClient. Cette valeur correspond généralement au nom du domaine enregistré qu'un serveur DNS associe à l'adresse IP du poste local faisant fonctionner le serveur, ou à un alias défini pour ce nom de domaine.

Dans certains cas, vous pouvez également choisir d'utiliser un nom de domaine par défaut à usage interne uniquement et non valide pour l'extérieur (par exemple "`company.mail`"). Si vous configurez votre serveur de cette façon, vous devrez peut-être utiliser l'outil Conversion d'en-têtes 62 et/ou le Dmoteur de remplacement de nom de domaine 77.

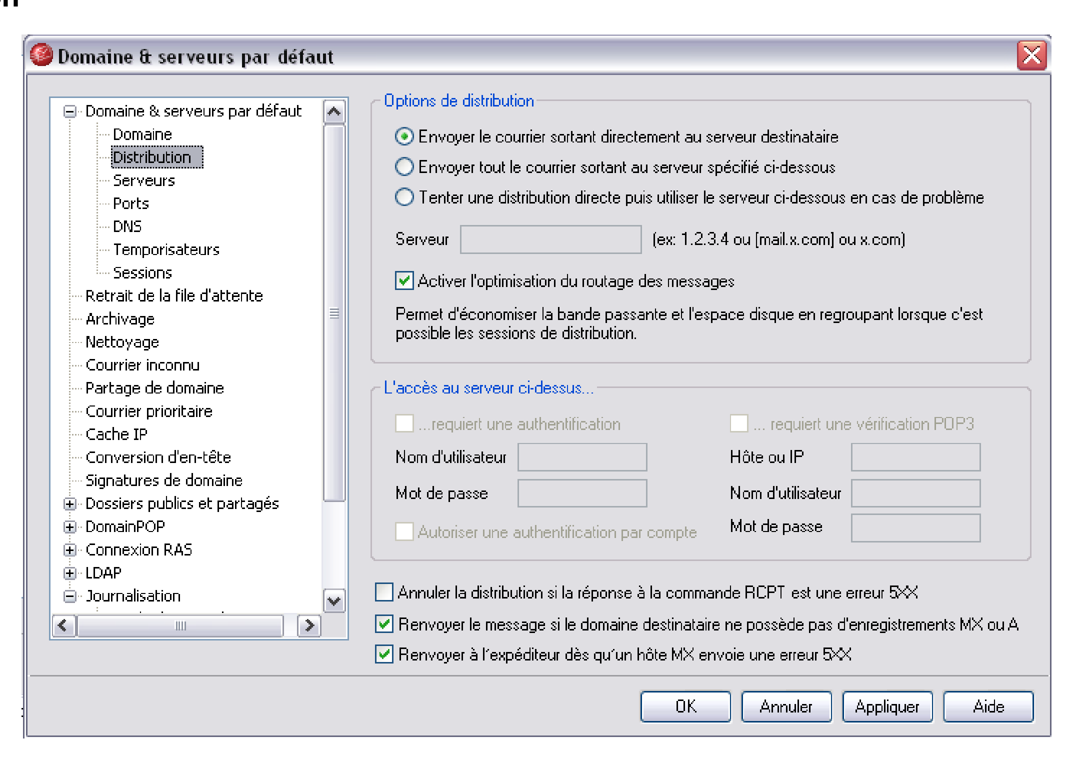
Nom de domaine complet (FQDN) de cet hôte
Ce nom de domaine est utilisé dans la commande SMTP HELO/EHLO lors de l’envoi de courrier. Dans la plupart des cas, il s’agit de votre nom de domaine par défaut. Il peut également être sous la forme "[1.2.3.4]".

IP du domaine
Adresse IP du domaine.

Limiter les connexions à cette IP uniquement
Si vous cochez cette option, MDaemon limite les connexions au domaine par défaut à l’IP spécifiée dans le champ ci-dessus. Il n’est généralement nécessaire d’utiliser cette option que dans certaines circonstances d’hébergement de plusieurs domaines.

Pour plus d’informations sur ce type de configuration, voir : **Hébergement de plusieurs domaines** 101

3.1.1.2 Distribution



Options de ditribution

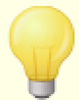
Envoyer le courrier sortant directement au serveur destinataire
En cochant cette case, MDaemon tente de distribuer l’ensemble du courrier directement, sans passer par un autre hôte. Il place les messages non distribuables dans le système de relance et renouvelle les tentatives de distribution en fonction des paramètres et intervalles de temps fixés dans la File de relance 430. Pour y

accéder, cliquez sur le menu "Files d'attente » Files d'attente... » File de relance".

Envoyer tout le courrier sortant au serveur spécifié ci-dessous
Sélectionnez cette option si vous souhaitez que tous les messages sortants, peu importe leur domaine de destination, soient envoyés vers un hôte ou un domaine chargé d'acheminer le courrier. Dans ce cas, tous les messages sortants seront envoyés à l'hôte spécifié dans le champ Serveur. En général, cette fonction n'est utile qu'en présence de gros volumes, lorsqu'une distribution directe du courrier pourrait entraîner une utilisation excessive des ressources du serveur. Si un message ne peut pas être distribué, il est placé dans le système de relance.

Tenter une distribution directe puis utiliser le serveur ci-dessous en cas de problème
Activez cette option si vous souhaitez envoyer uniquement le courrier sortant non distribuable vers l'hôte ou le domaine indiqué dans le champ *Serveur* (voir ci-dessous). Le courrier non distribuable est généralement destiné soit à des hôtes qui ne peuvent pas être résolus en adresse IP effective (comme une passerelle non enregistrée vers un réseau distant), soit à des hôtes résolus correctement, mais auxquels il est impossible de se connecter directement, ou qui refusent les connexions directes. Avec cette option, le courrier est transmis par MDaemon à un MTA plus puissant, au lieu d'être renvoyé à son destinataire. Parfois, le système de messagerie exécuté par votre FAI possède des techniques d'acheminement du courrier auxquelles votre serveur local peut ne pas avoir accès directement. Si un message ne peut ni être distribué directement, ni transmis à l'hôte ou au domaine de relais, il est déplacé dans la file de relance et MDaemon essaie à nouveau de le distribuer, en fonction des paramètres la File de relance 430. À chaque nouvelle tentative, MDaemon essaie d'abord de distribuer le message directement avant le transmettre à l'hôte ou au domaine de relais.

Serveur
Entrez le nom de domaine ou l'adresse IP de votre hôte de messagerie ou de votre FAI dans ce champ. Il s'agit en principe du serveur SMTP de votre FAI.



N'indiquez ni l'adresse IP, ni le nom du domaine par défaut de MDaemon. La valeur doit désigner un FAI ou à un autre serveur de messagerie qui pourra relayer le courrier à sa place.

Activer l'optimisation du routage des messages
Par défaut, lorsque c'est possible MDaemon conserve une seule copie des messages ayant plusieurs destinataires et utilise ensuite des commandes RCPT pour distribuer le message. Cela permet d'économiser de l'espace disque et de la bande passante. Cette option est utile si par exemple un même message est destiné à plusieurs utilisateurs du domaine. De plus, si vous utilisez l'option de distribution envoyant tout le courrier sortant à une IP/un domaine/un hôte spécifique, MDaemon conserve une seule copie de chaque message et utilise plusieurs commandes RCPT même lorsque les destinataires appartiennent à des domaines différents.

L'accès au serveur ci-dessus...

Par mesure de sécurité, certains FAI ou hôtes de relais exigent une authentification ou une vérification POP pour pouvoir se connecter et envoyer du courrier via leurs

serveurs. Si votre FAI ou hôte de messagerie exige une authentification ou une vérification POP, cochez l'option correspondante et saisissez vos identifiants de connexion.

...requiert une authentification
Si votre FAI ou l'hôte de relais exige une authentification, cochez cette option et indiquez votre nom d'utilisateur et votre mot de passe. Ces identifiants seront utilisés dans tous les messages SMTP sortants envoyés au serveur spécifié ci-dessus. Vous pouvez également indiquer un identifiant spécifique pour chaque compte à l'aide de l'option *Autoriser une authentification par compte*. Dans ce cas, indiquez l'identifiant dans les paramètres de chaque compte, onglet Informations générales 301.

Nom d'utilisateur
Saisissez ici votre nom d'utilisateur ou identifiant.

Mot de passe
Mot de passe pour la connexion à votre FAI ou hôte de relais.

...requiert une vérification POP3
Si votre FAI ou l'hôte de relais exige une authentification POP, cochez cette option et indiquez votre nom d'utilisateur et votre mot de passe.

Hôte ou IP
Hôte ou adresse IP du serveur de relais.

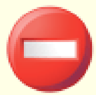
Nom d'utilisateur
Saisissez ici votre nom d'utilisateur ou identifiant du compte POP.

Mot de passe
Mot de passe correspondant.

Autoriser une authentification par compte
Cochez cette option si vous souhaitez autoriser chaque compte à s'authentifier individuellement lors de l'envoi de messages SMTP par le biais d'un hôte de relais. Au lieu d'employer le nom d'utilisateur indiqué ci-dessus, MDaemon utilise les valeurs *Identifiants pour l'hôte de relais* figurant dans l'onglet Informations générales 301 de l'Éditeur de comptes. Si ce champ n'est pas rempli, MDaemon utilise les valeurs ci-dessus.

Si vous souhaitez que pour cette authentification le compte utilise son mot de passe MDaemon au lieu de celui de l'hôte de relais, modifiez le fichier `MDaemon.ini` comme suit :

```
[AUTH]
ISPAUTHUsePasswords=Yes (pae défaut : No)
```



Si vous configurez `ISPAUTHUsePasswords=Yes` les mots de passe de vos comptes locaux seront transmis à l'hôte de relais. Ceci est donc fortement déconseillé car ces informations peuvent mettre en danger votre système de messagerie. N'effectuez cette opération que si elle est requise par un hôte de relais en qui vous avez entièrement confiance. De plus, si vous utilisez cet paramètre et que vous autorisez les utilisateurs à modifier leur mot de passe ; lorsqu'un utilisateur change le mot de passe de son compte cela modifie également celui de l'hôte de relais. Cela peut entraîner des échecs d'authentification si le mot de passe est changé au niveau du compte mais pas au niveau de l'hôte.

Annuler la distribution si réponse à la commande RCPT est une erreur 5XX

Activez cette option si vous souhaitez que MDaemon abandonne la distribution d'un message lorsque la réponse à la commande RCPT est une erreur fatale 5xx. Cette option est désactivée par défaut.

Renvoyer le message si le domaine destinataire ne possède pas d'enregistrements A ni MX

Cochez cette option pour que MDaemon renvoie immédiatement le message lorsque les vérifications DNS indiquent que le domaine du destinataire ne possède pas d'enregistrement MX ni A. Cela évite que des messages ne passent inutilement dans le cycle des tentatives de distribution.

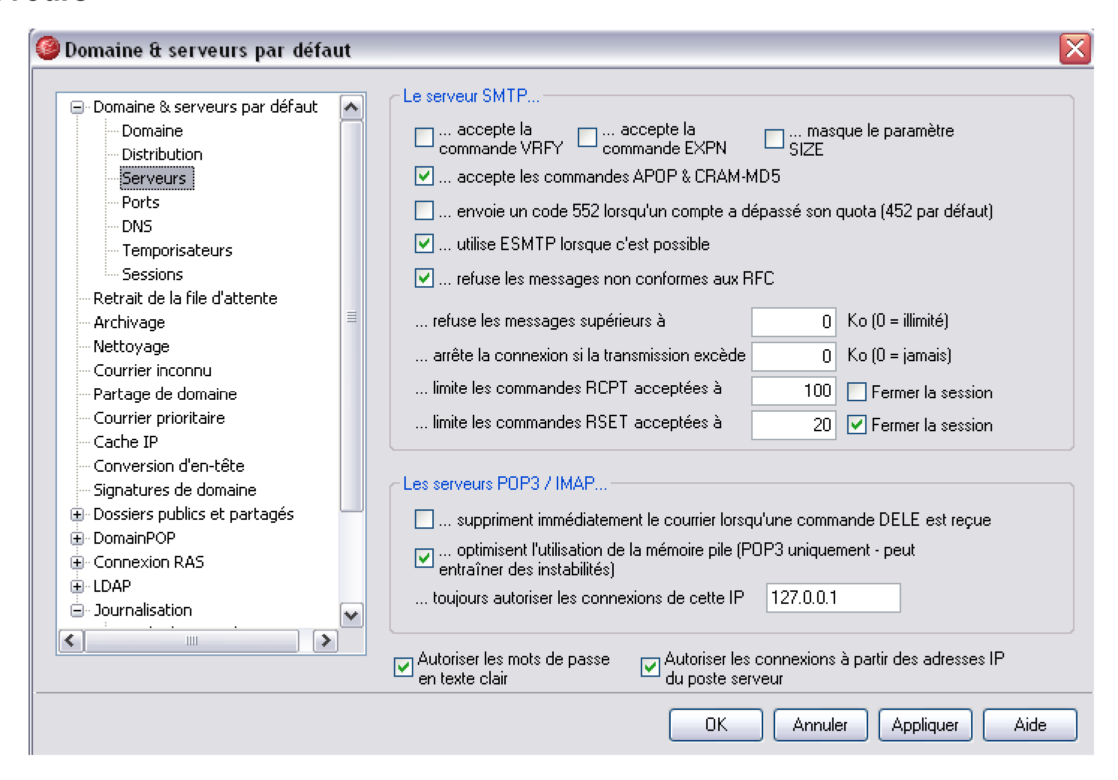
Renvoyer à l'expéditeur dès qu'un hôte MX envoie une erreur 5XX

Lorsque cette option est activée, MDaemon renvoie le message à l'expéditeur dès qu'il reçoit un code d'erreur 5xx d'un hôte MX. Par conséquent, il n'essaie pas de distribuer le message aux hôtes MX suivants pouvant exister sur le domaine du destinataire. Si cette option n'est pas activée, MDaemon ne renvoie pas le message à l'expéditeur tant qu'au moins un des hôtes MX renvoie un code 4xx (erreur temporaire). Cette option est désactivée par défaut.

Voir également :

File de relance 430

3.1.1.3 Serveurs



Le serveur SMTP...

...accepte la commande VRFY
Activez cette option si vous souhaitez répondre aux commandes SMTP VRFY. Elle est parfois utilisée par des serveurs envoyant des commandes SMTP call forward ou call back afin de vérifier la validité d'une adresse e-mail. Cette fonctionnalité est désactivée par défaut.

...accepte la commande EXPN
Activez cette option si vous souhaitez répondre aux commandes EXPN.

...masque le paramètre SIZE
Activez cette option si vous souhaitez que le paramètre de commande ESMTP SIZE soit masqué.

...accepte les commandes APOP & CRAM-MD5
Par défaut, MDaemon accepte les méthodes d'authentification APOP et CRAM-MD5. Ces méthodes fournissent une couche de sécurité supplémentaire en permettant aux utilisateurs de s'authentifier sans devoir envoyer des mots de passe en texte clair.

...envoie un code 552 lorsqu'un compte a dépassé son quota (452 par défaut)
Cette option envoie un code d'erreur permanente 552 ("Action annulée : manque de ressources de stockage") lorsqu'un message est adressé à un compte ayant dépassé son quota 317. Par défaut, la réponse envoyée est le code d'erreur temporaire 452 ("Action non effectuée : manque de ressources système").

...utilise ESMTP lorsque c'est possible
Lorsque cette option est activée, MDaemon accepte les commandes "extended SMTP".

...refuse les messages non conformes aux RFC
Activez cette option si vous souhaitez refuser pendant la session SMTP les messages n'étant pas conformes aux standards des RFC. Pour être conforme, un message doit :

1. Être d'une taille supérieure à 32 octets (taille minimum nécessaire pour inclure tous les éléments requis).
2. Posséder un en-tête DATE:.
3. Posséder un en-tête FROM: ou bien SENDER:.
4. Ne pas comporter plus d'un en-tête FROM:.
5. Ne pas comporter plus d'un en-tête SUBJECT: (l'en-tête SUBJECT: n'est pas obligatoire).

Cette vérification ne s'applique pas aux messages provenant de sessions authentifiées ou de domaines/d'IP autorisés.

...refuse les messages supérieurs à [xx] Ko (0=pas de limite)
Lorsque cette option est activée, MDaemon refuse ou ne traite pas le courrier distribué par SMTP qui excède la taille indiquée. Dans ce cas, MDaemon tente d'utiliser la commande ESMTP SIZE (définie dans la RFC-1870). Si l'agent expéditeur prend en charge cette extension SMTP, MDaemon détermine la taille du message avant sa distribution et le refuse si elle est supérieure à la taille indiquée. Si l'agent expéditeur ne prend pas en charge cette extension SMTP, MDaemon accepte le message, vérifie après le transfert, et enfin refuse éventuellement de le distribuer une fois la transaction terminée.

...arrête la connexion si la transmission excède [xx] Ko (0=jamais)
Si la transmission de données durant une connexion dépasse ce seuil, MDaemon ferme la connexion.

...limite les commandes RCPT acceptées à [xx] (100 d'après la RFC)
Utilisez cette option si vous souhaitez limiter le nombre de commandes RCPT pouvant être contenues dans un messages.

Fermer la session
Cochez cette case si vous souhaitez fermer la session dès que le nombre maximum de commandes RCPT autorisé est atteint.

...limite les commandes RSET acceptées à [xx]
Utilisez cette option si vous souhaitez limiter le nombre de commandes RSET autorisées dans une session SMTP (par défaut : 20).

Fermer la session
Cochez cette case si vous souhaitez fermer la session dès que le nombre

maximum de commandes RSET autorisé est atteint.

Les serveurs POP3 / IMAP

...suppriment immédiatement le courrier lorsqu'une commande DELE est reçue
Activez cette option si vous souhaitez que MDaemon supprime immédiatement les messages retirés par un utilisateur même si la session POP n'est pas terminée correctement.

...optimisent l'utilisation de la mémoire pile (POP3 uniquement - peut entraîner des instabilités)
Cette option maximise l'utilisation de la mémoire pile par MDaemon afin d'éviter les problèmes pouvant survenir lorsque des comptes POP actifs contiennent des milliers de messages. Si vous désactivez cette option, le serveur POP sera plus conservateur mais l'interface risque de mettre du temps à répondre lorsque le serveur POP est surchargé.

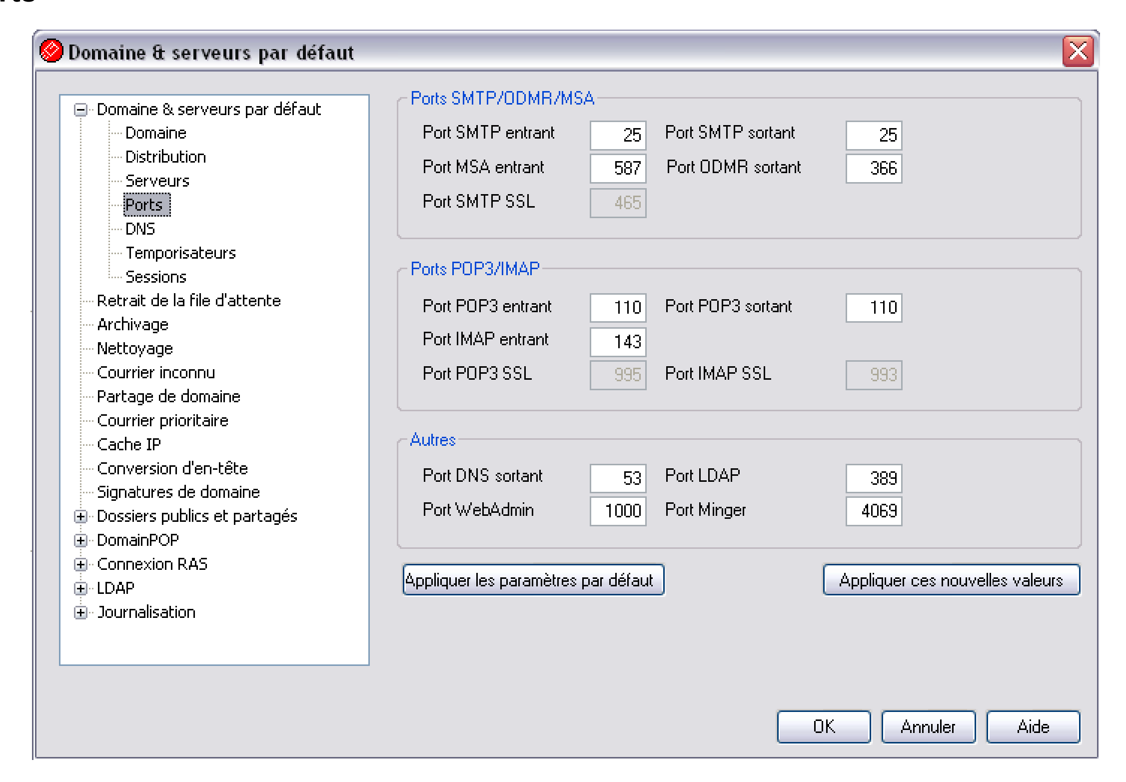
...toujours autoriser les connexions de cette IP
Les serveurs POP et IMAP acceptent toujours les connexions depuis les adresses IP indiquées dans ce champ sans tenir compte des paramètres du Bouclier et de l'Écran IP.

—

Autoriser les mots de passe en texte clair
Cette option détermine si les mots de passe envoyés en texte clair aux serveurs SMTP, IMAP, ou POP3 sont acceptés. Si elle est désactivée, les commandes POP3 USER, POP3 PASS, IMAP LOGIN, IMAP AUTH LOGIN, et SMTP AUTH LOGIN ne fonctionneront que si la session utilise une connexion SSL.

Autoriser les connexions à partir des adresses IP du poste serveur
Lorsque cette option est activée, MDaemon peut se connecter à lui-même.

3.1.1.4 Ports

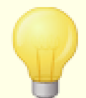


Ports SMTP / ODMR / MSA (certaines fonctionnalités nécessitent MDaemon PRO)

Port SMTP entrant
Port TCP écouté par MDaemon pour les connexions entrantes des clients SMTP. Il est généralement conseillé de conserver la valeur par défaut.

Port SMTP sortant
Port utilisé pour l'envoi de courrier à d'autres serveurs SMTP.

Port MSA entrant
Le port MSA (Message Submission Agent) est une alternative au port SMTP. L'authentification est obligatoire sur ce port. Par conséquent, les utilisateurs doivent s'assurer que leur client de messagerie est configuré de façon à utiliser des connexions authentifiées. De plus, ce port peut s'avérer utile pour les usagers distants si votre FAI bloque le port 25. Si vous ne souhaitez pas indiquer de port MSA, saisissez "0" dans ce champ.



Les connexions sur le port MSA ne sont pas soumises aux vérifications PTR et inverse, à l'Écran IP et l'Écran d'hôte, ni au Bouclier IP et au système de répulsion. Elles sont toutefois protégées contre les attaques dictionnaire.

Port ODMR entrant
MDaemon écoute ce port pour les connexions ODMR, telles que les connexions ATRN à partir de passerelles de domaine.

Port SMTP SSL
Il s'agit du port dédié pour les sessions SMTP qui utilisent une connexion SSL (Secure Sockets Layer). Voir SSL & Certificats 271 pour en savoir plus.

Ports POP3 / IMAP (certaines fonctionnalités nécessitent MDaemon PRO)

Port POP3 entrant
MDaemon écoute ce port pour les connexions entrantes à partir de clients POP distants.

Port POP3 sortant
Ce port est utilisé pour le retrait du courrier sur des serveurs POP3.

Port IMAP entrant
MDaemon écoute ce port pour les requêtes IMAP entrantes.

Port POP3 SSL
Il s'agit du port dédié pour les clients de messagerie POP3 qui utilisent une connexion SSL (Secure Sockets Layer). Voir SSL & Certificats 271 pour en savoir plus.

Port IMAP SSL
Il s'agit du port dédié pour les clients de messagerie IMAP qui utilisent une connexion SSL (Secure Sockets Layer). Voir SSL & Certificats 271 pour en savoir plus.

Autres

Port DNS sortant
Indiquez le port que MDaemon doit utiliser pour recevoir et envoyer des paquets de données vers le serveur DNS.

Port LDAP
MDaemon envoie des informations de la base de données et du carnet d'adresses à votre serveur LDAP sur ce port.

Voir : Support LDAP 89

Port WebAdmin
MDaemon écoute ce port pour les connexions WebAdmin 129.

Port Minger
Port écouté par le serveur Minger 369.

Appliquer les paramètres par défaut
Cliquez sur ce bouton pour rétablir toutes les valeurs par défaut.

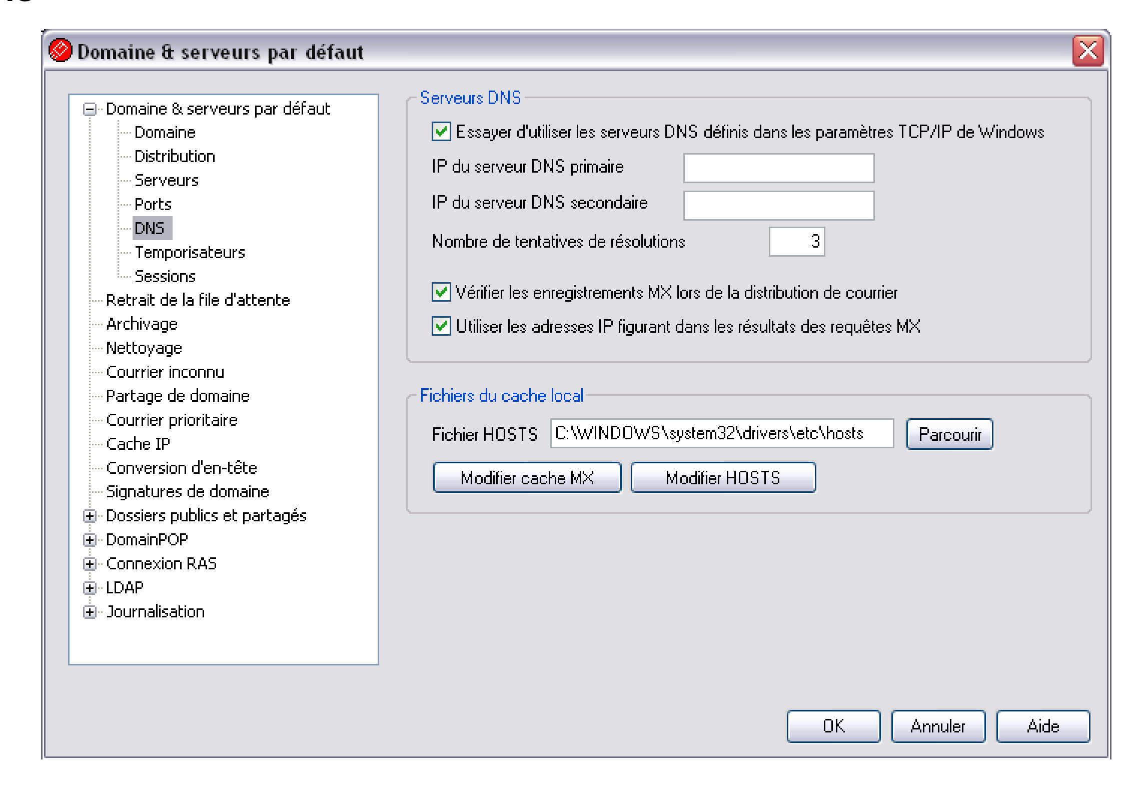
Appliquer ces nouvelles valeurs
Lorsque vous modifiez la valeur d'un paramètre, vous devez cliquer sur ce bouton pour que vos changements prennent effet immédiatement. Sinon, ils ne sont pris en compte qu'au démarrage suivant du serveur.



Ces paramètres sont déterminants pour un fonctionnement correct du serveur. Vous ne devez pas les modifier, à moins d'être certain de devoir le faire. Savoir paramétrer les ports dont MDaemon se sert vous permettra de configurer le serveur de sorte qu'il fonctionne avec des proxy ou d'autres logiciels nécessitant des ports spécifiques.

Une adresse IP (une machine) ne dispose que d'un seul des ports disponibles. Si un autre programme tente d'accéder à un port déjà utilisé par un autre logiciel, un message d'erreur informera l'utilisateur que l'adresse demandée (IP : PORT) est déjà en cours d'utilisation.

3.1.1.5 DNS



Serveurs DNS

Essayer d'utiliser les serveurs DNS définis dans les paramètres TCP/IP de Windows
Windows conserve parfois l'adresse IP d'un serveur DNS dans les paramètres TCP/IP. Si c'est le cas sur votre ordinateur, vous pouvez alors activer cette option. Si MDaemon ne parvient pas à trouver un serveur DNS défini localement, il poursuivra et utilisera ceux indiqués dans cette boîte de dialogue.

IP du serveur DNS primaire
Indiquez l'adresse IP du serveur DNS que MDaemon doit interroger pour les

enregistrements A et MX.

IP du serveur DNS secondaire
Indiquez l'adresse IP du serveur DNS secondaire.

Nombre de tentatives de résolution
Si une tentative de résolution d'IP échoue, MDaemon répètera cette tentative le nombre de fois indiqué dans ce champ. Si vous avez spécifié un serveur DNS secondaire, les deux serveurs seront interrogés à chaque tentative de résolution.

Vérifiez les enregistrements MX lors de la distribution de courrier
Activez cette option si vous voulez que MDaemon interroge les serveurs DNS indiqués ci-dessus sur les enregistrements MX lorsqu'il essaie d'envoyer du courrier.



Lorsque vous indiquez un hôte auquel le courrier doit être transféré, copié, ou envoyé,saisissez son nom entre crochets [ ] pour ne pas effectuer de vérification MX lors de la distribution. Par exemple, si vous indiquez 'altn.com' les vérifications MX sont effectuées normalement, mais si vous indiquez '[altn.com]', seuls les enregistrements A sont vérifiés. Cette option est globale et s'applique à toutes les fonctionnalités de MDaemon.

Utiliser les adresses IP figurant dans les résultats des requêtes MX
Cochez cette case pour que MDaemon tente l'envoi aux adresses IP des enregistrements A, lorsque celles-ci sont découvertes au cours du traitement de l'enregistrement MX.

Fichiers du cache local

Fichier Hosts...
Avant d'interroger les serveurs DNS, MDaemon tente de résoudre les adresses à l'aide du fichier HOSTS de Windows. Si ce fichier contient l'adresse IP du domaine en question, MDaemon n'aura pas besoin d'interroger le serveur DNS.



Vous devez saisir le chemin complet et le nom de ficher au lieu du seul nom de fichier. MDaemon essaiera d'utiliser la valeur suivante comme emplacement par défaut de ce fichier :

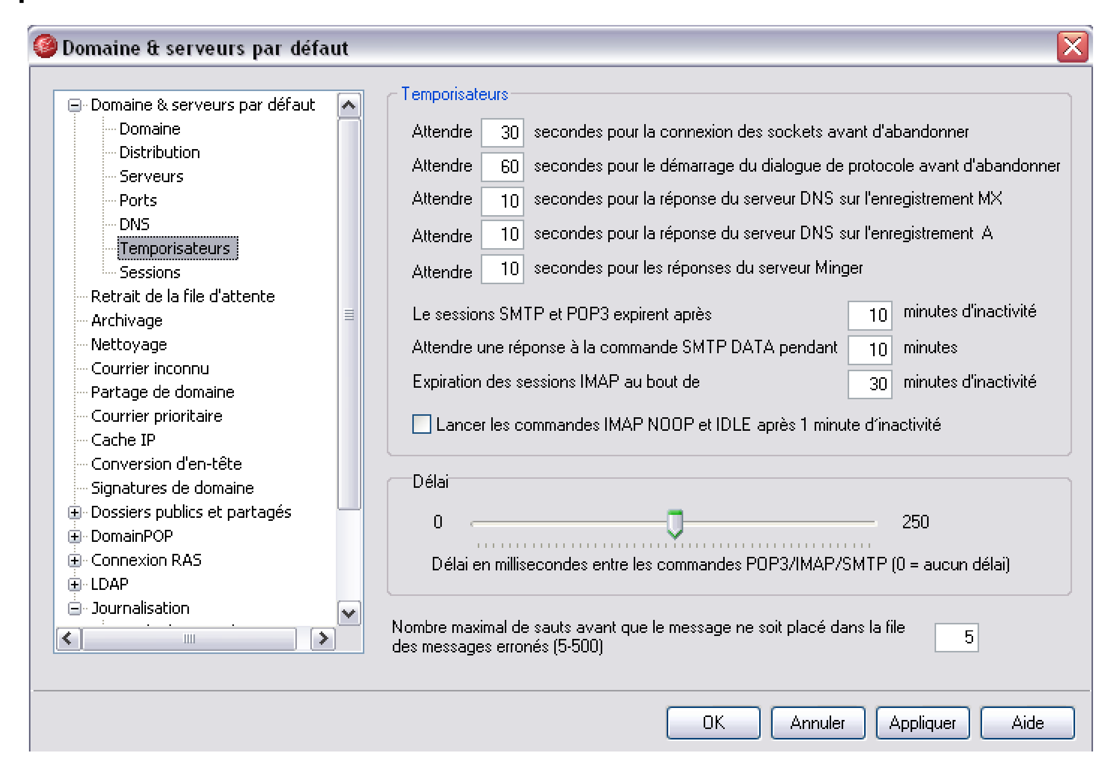
[lettre du lecteur]:\windows\system32\drivers\etc\hosts

Le fichier HOSTS est un fichier Windows qui contient l'adresse IP primaire ou celle de l'enregistrement A pour les noms de domaine. MDaemon vous permet également d'indiquer des adresses IP de l'enregistrement MX dans un fichier nommé MXCACHE.DAT. Ce fichier se trouve dans le sous-répertoire MDaemon\APP\. Chargez le fichier MXCACHE.DAT dans un éditeur de texte et lisez les remarques en haut du fichier pour obtenir davantage d'informations.

Modifier cache MX
Cliquez sur ce bouton pour afficher ou modifier le fichier MXCACHE.DAT dans un éditeur de texte.

Modifier HOSTS
Cliquez sur ce bouton pour afficher ou modifier le fichier HOSTS dans un éditeur de texte.

3.1.1.6 Temporisateurs



Temporisateurs

Attendre XX secondes pour la connexion des sockets avant d'abandonner
Après avoir lancé une requête de connexion, MDaemon attend le nombre de secondes indiqué pour que le système distant accepte la connexion. S'il ne répond pas avant la fin de ce délai, MDaemon envoie le courrier soit à l'hôte passerelle, soit à la file de relance, en fonction de l'option que vous avez choisie dans l'onglet Domaine 33.

Attendre XX secondes pour le démarrage du dialogue de protocole avant d'abandonner
Dès qu'une connexion est établie avec un hôte distant, MDaemon attend le nombre de secondes indiqué pour que le serveur distant commence le dialogue SMTP ou POP3. Si l'hôte distant ne commence pas la session de protocole pendant cet intervalle, MDaemon envoie le courrier soit à l'hôte passerelle, soit à la file de relance, en fonction de l'option que vous avez choisie dans l'onglet Domaine 33.

Attendre XX secondes pour la réponse du serveur DNS sur l'enregistrement MX
MDaemon attend les réponses à ses requêtes MX durant le nombre de secondes indiqué. Si le serveur DNS ne répond pas avant la fin de ce délai, MDaemon essaie d'envoyer le courrier à l'adresse IP spécifiée dans l'enregistrement DNS A de l'hôte distant. Si cette tentative échoue, MDaemon envoie le courrier soit à l'hôte passerelle, soit à la file de relance, en fonction de l'option que vous avez choisie dans l'onglet Domaine.33

Attendre XX secondes pour la réponse du serveur DNS sur l'enregistrement A
Ce temporisateur régit la durée pendant laquelle MDaemon attend, en essayant de résoudre l'adresse IP d'un hôte distant. Si la tentative échoue, MDaemon envoie le courrier soit à l'hôte passerelle, soit à la file de relance, en fonction de l'option que vous avez choisie dans l'onglet Domaine33.

Attendre XX secondes pour les réponses du serveur Minger
Nombre maximum de secondes pendant lequel MDaemon attend une réponse d'un serveur Minger369.

Les sessions SMTP et POP3 expirent après XX minutes d'inactivité
Si une session connectée avec succès reste inactive pendant la durée indiquée, MDaemon abandonne la transaction. Il la renouvelle au cycle suivant de traitement du courrier.

Attendre une réponse à la commande SMTP DATA pendant X minutes
Indique la durée pendant laquelle MDaemon attend la réponse "250 Ok" après avoir envoyé la commande DATA au cours de la session SMTP. En effet, si le serveur destinataire doit effectuer des analyses anti-spam, anti-virus, etc., cette option permet de lui laisser le temps nécessaire pour effectuer ces opérations. Valeur par défaut : 10 minutes.

Expiration des sessions IMAP au bout de XX minutes d'inactivité
Si une session IMAP reste inactive durant le laps de temps indiqué, MDaemon ferme la session.

Lancer les commandes IMAP NOOP et IDLE après 1 minute d'inactivité
Si cette case est cochée, le temporisateur d'inactivité IMAP est fixé à une minute lorsqu'une commande NOOP est reçue. Certains clients IMAP lancent des commandes NOOP uniquement pour affirmer qu'une session est ouverte, alors qu'aucune transaction de courrier n'est en cours. Cette fonctionnalité évite que de telles sessions restent actives et limitent, par conséquent, les ressources utilisées. Elle est particulièrement utile pour des sites de messagerie IMAP volumineux.

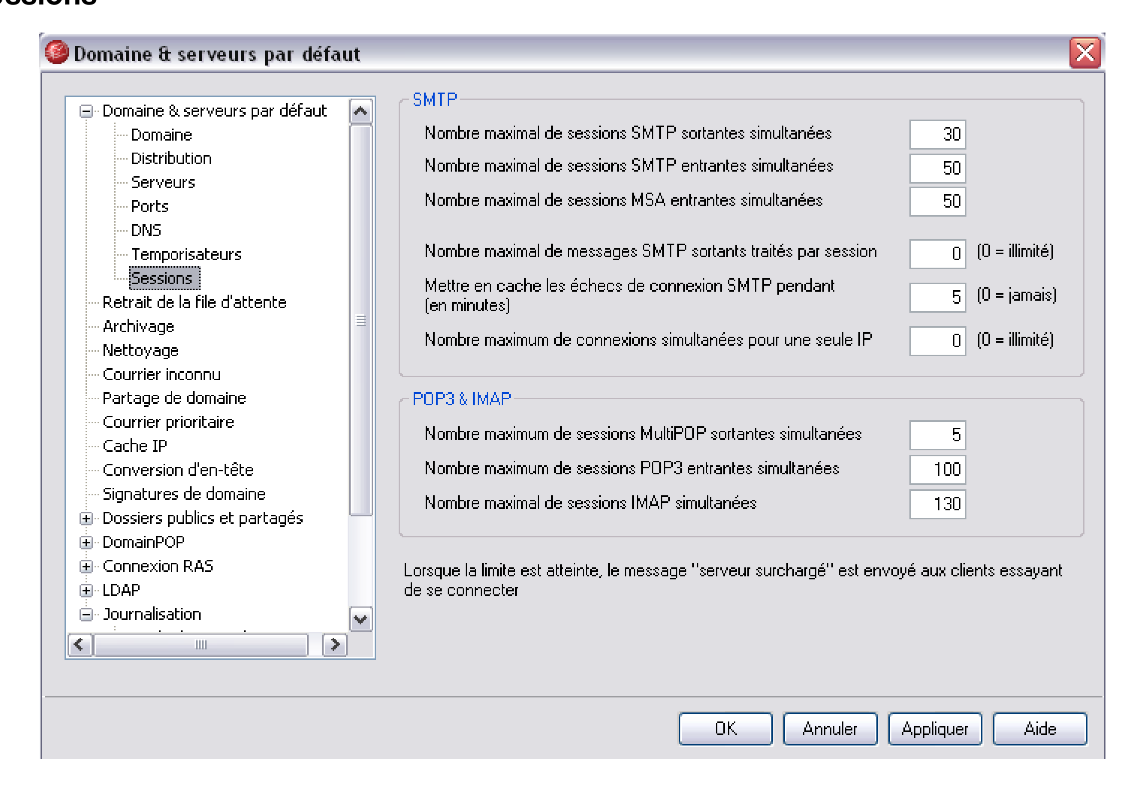
Délai d'attente

Délai d'attente – xx millisecondes
Il s'agit du délai en millisecondes entre les commandes POP/SMTP/IMAP. Il permet d'éviter que les connexions à haut débit ne traitent les données plus vite que le destinataire ne peut les extraire. Ce délai ne prend effet que lors de l'envoi de commandes POP/SMTP/IMAP – le transfert réel d'un fichier de messages est déjà mis en totalité dans la mémoire tampon.

Détection et contrôle de boucle

Nombre maximal de sauts de message avant que le message ne soit placé dans la file des messages erronés (5-500)
Les standards RFC stipulent qu'un serveur de messagerie doit marquer chaque message à chaque fois qu'il le traite. Ces marqueurs peuvent être dénombrés et utilisés comme mesure de sécurité provisoire contre les boucles de messages parfois provoquées par des configurations incorrectes. S'ils ne se sont pas détectés, ces cycles de distribution en boucle utilisent toutes vos ressources. En dénombrant le nombre de traitements de chaque message, il est possible de détecter les e-mails problématiques et de les placer dans le répertoire des messages erronés. Si le courrier n'a pas atteint son destinataire après avoir été traité par un certain nombre de serveurs, on suppose qu'une boucle de message est en cours. La valeur par défaut de ce paramètre est suffisante pour empêcher les boucles de messages. Il n'est pas nécessaire de la modifier.

3.1.1.7 Sessions



SMTP

Nombre maximal de sessions SMTP sortantes simultanées
La valeur saisie ici représente le nombre maximal de sessions SMTP sortantes qu'il est possible de créer au moment d'envoyer du courrier. Chaque session enverra des messages sortants jusqu'à ce que la file d'attente soit pleine ou que la valeur dans le champ *Nombre maximal de messages SMTP sortants traités par session* soit atteinte. Par exemple, si la file d'attente des messages sortants contient vingt messages en attente d'envoi, et que la valeur indiquée dans ce champ est cinq, cinq

sessions seront ouvertes simultanément et chacune d'entre elles enverra consécutivement quatre messages.

Déterminez le nombre de sessions offrant la meilleure performance pour votre bande passante. Il est possible d'autoriser un très grand nombre de sessions, mais votre bande passante pourrait être surchargée ou votre ordinateur pourrait ne plus avoir de ressources, ce qui entraînerait une perte d'efficacité pour la distribution du courrier. Souvenez-vous que chaque session SMTP créée par MDaemon distribue du courrier consécutivement. Par conséquent, quatre sessions distribuant deux messages chacune devraient fonctionner mieux et plus vite que huit sessions ne distribuant qu'un message chacune.

Nombre maximal de sessions SMTP entrantes simultanées
Cette valeur correspond au nombre de sessions SMTP entrantes simultanées que le serveur accepte avant de renvoyer le message "Serveur surchargé".

Nombre maximal de sessions MSA entrantes simultanées
Indiquez ici le nombre maximal de sessions mail submission agent (MSA) entrantes simultanées autorisées.

Nombre maximal de messages SMTP sortants traités par session
Ce paramètre correspond au nombre maximal de messages individuels envoyés à chaque session, avant que ces envois soient stoppés pour libérer de la mémoire. Normalement, vous devez laisser la valeur 0 dans ce champ. Ainsi, chaque session continuera de distribuer le courrier, jusqu'à ce que la file d'attente soit vide.

Mettre en cache les échecs de connexion SMTP pendant (en minutes) (0 = jamais)
Lorsqu'une connexion SMTP avec un hôte échoue, MDaemon abandonne les tentatives de connexion pendant le nombre de minutes indiqué. Cela évite qu'en cas de problème MDaemon essaie inutilement de se connecter à de multiples reprises au même hôte lorsque plusieurs messages lui sont destinés. La valeur par défaut est de 5 minutes. Indiquez 0 si vous ne souhaitez pas mettre en cache les échecs de connexion SMTP.

Nombre maximum de connexions simultanées pour une seule IP (0 = illimité)
Utilisez cette option pour limiter le nombre de connexions simultanées autorisées pour une seule IP lors de la distribution du courrier. Indiquez 0 si vous ne souhaitez pas limiter les connexions simultanées.

Cela peut s'avérer utile pour empêcher qu'un trop grand nombre de connexions soient effectuées simultanément. Si la distribution d'un message nécessitant la connexion à une IP excède cette limite, la connexion n'est pas effectuée et l'hôte MX (ou hôte de relais) suivant est utilisé. Si aucun hôte supplémentaire n'est disponible, le message est remis en file d'attente jusqu'au prochain cycle de distribution. Cette option est désactivée par défaut afin de conserver le fonctionnement existant. De plus, cette fonctionnalité ne s'applique pas aux connexions à des IP autorisées. Si vous souhaitez toutefois l'appliquer, modifiez le fichier `MDaemon.ini` comme suit :

```
[Sessions]
TrustedIPsUseConnectionLimit=Yes (par défaut : No)
```

Elle ne s'applique également pas aux connexions d'IP locales : 127.0.0., 192.168., 10., et 172.16.0.0/12. Pour l'appliquer aux IP locales, modifiez le fichier `MDaemon.ini` comme suit :

```
[Sessions]
ReservedIPsUseConnectionLimit=Yes (par défaut : No)
```

POP3 & IMAP

Nombre maximal de sessions MultiPOP sortantes simultanées

La valeur saisie ici représente le nombre maximal de sessions POP sortantes pouvant être créées lors de la collecte du courrier MultiPOP. Chaque session recevra ce type de courrier jusqu'à ce que tous les serveurs MultiPOP aient été traités et que l'ensemble du courrier ait été collecté. Par exemple, s'il y a quinze sessions MultiPOP parmi toutes celles ouvertes par vos utilisateurs, et que la valeur de ce paramètre est trois, chaque session reçoit alors du courrier à partir de cinq sources MultiPOP.

Déterminez le nombre de sessions produisant la meilleure performance pour votre bande passante. Comme il est possible d'autoriser un très grand nombre de sessions, votre bande passante peut être surchargée et votre ordinateur ne plus avoir de ressources, ce qui diminuerait l'efficacité de la distribution du courrier. Souvenez-vous que chaque session POP créée par MDaemon reçoit du courrier jusqu'à ce que toutes les ressources soient épuisées. Par conséquent, quatre sessions recevant du courrier à partir de vingt sources peuvent fonctionner mieux et plus vite que vingt sessions recevant du courrier à partir d'une seule source.

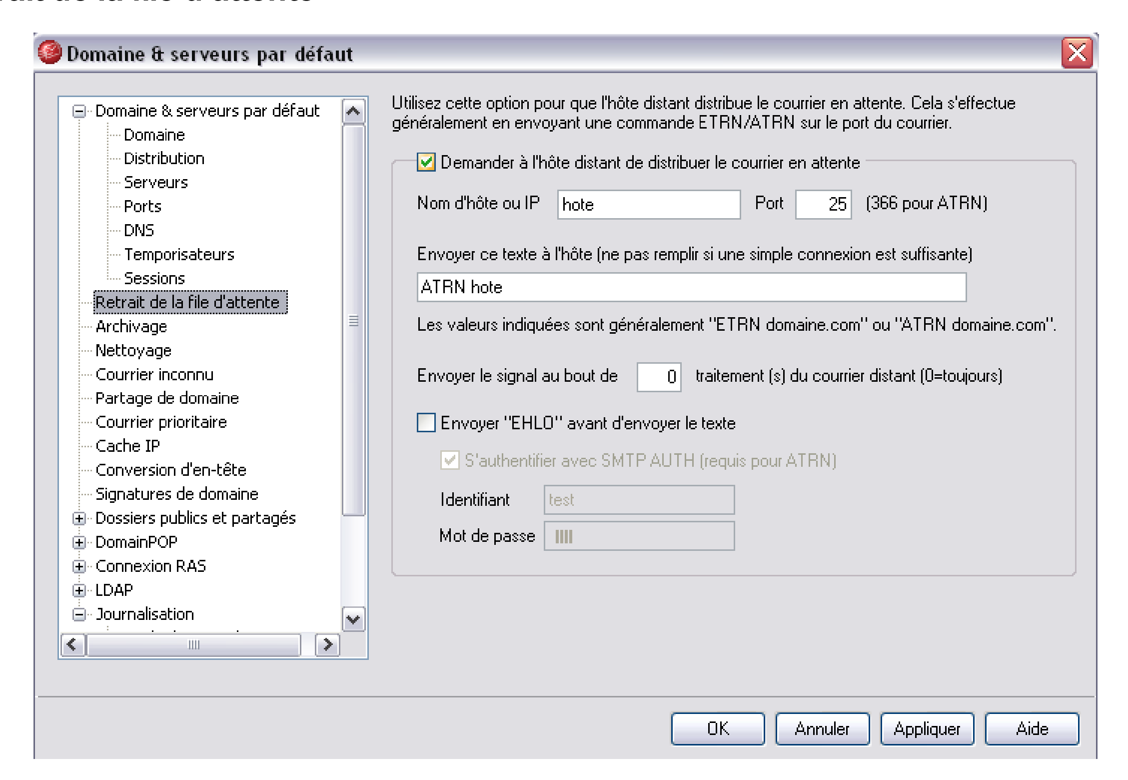
Nombre maximal de sessions POP entrantes simultanées

Cette valeur correspond au nombre maximal de sessions POP entrantes et simultanées que le serveur accepte avant de renvoyer le message "Serveur surchargé".

Nombre maximal de sessions IMAP entrantes simultanées

Cette valeur correspond au nombre maximal de sessions IMAP simultanées que le serveur accepte avant de renvoyer le message "Serveur surchargé".

3.1.2 Retrait de la file d'attente



Demander à l'hôte distant de distribuer le courrier en attente
Lors du traitement du courrier distant, MDaemon peut se connecter à n'importe quel serveur sur n'importe quel port et envoyer la chaîne de votre choix. Cette fonction est utile lorsque vous voulez signaler à un serveur distant que vous retirez du courrier en lui envoyant une chaîne de caractères. Par exemple, ATRN, ETRN ou QSND. Vous pouvez également utiliser cette fonctionnalité lorsqu'une session FINGER ou TELNET est nécessaire de façon ponctuelle, pour que votre FAI détecte que vous êtes connecté.

Nom d'hôte ou IP
Hôte auquel vous souhaitez vous connecter pour signaler le retrait de votre courrier

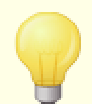
Port
Saisissez le port auquel vous souhaitez vous connecter. Par défaut, le port 25 (le port SMTP) convient à la méthode de signal ETRN ou QSND. Le port 366 est habituellement utilisé pour ATRN, et le port 79 pour FINGER.

Envoyer ce texte à l'hôte (ne pas remplir si une simple connexion est suffisante)
Indiquez la chaîne de texte qui doit être envoyée afin que votre courrier soit retiré. Par exemple, la méthode ETRN requiert le texte "ETRN" suivi du nom de domaine du site en file d'attente. D'autres méthodes requièrent l'envoi d'un texte différent. Consultez votre FAI si vous avez besoin d'informations complémentaires concernant les chaînes à envoyer pour déverrouiller votre file d'attente de courrier. Si vous avez la possibilité de choisir la méthode, il est recommandé d'utiliser On-Domain Mail Relay (ODMR) 51. ODMR requiert l'utilisation de la commande ATRN.

Envoyer le signal au bout de [xx] traitement(s) du courrier distant (0=toujours)
Par défaut, le signal de retrait de la file d'attente est envoyé à chaque traitement du courrier distant. Saisissez une valeur dans ce champ si vous souhaitez qu'il soit envoyé uniquement tous les XX traitements.

Envoyer "EHLO" avant d'envoyer le texte
Si vous activez cette option, le serveur auquel vous vous connecter doit être un serveur SMTP. Cette option permet l'ouverture d'une session SMTP et l'envoi de la commande SMTP "EHLO" avant l'envoi de la chaîne de déverrouillage.

S'authentifier avec SMTP AUTH (requis pour ATRN)
Par mesure de sécurité, certains FAI demandent à leurs clients de s'authentifier avec ESMTP AUTH avant d'envoyer le signal de retrait de la file d'attente ; cela évite que des utilisateurs non autorisés retirent leur courrier de la file. Si tel est le cas, cochez cette case puis saisissez les informations requises.



Vous devez vous authentifier lorsque vous utilisez la commande ATRN pour retirer votre courrier de la file d'attente.

Identifiant
Si vous devez vous identifier avant l'envoi du signal de retrait du courrier de la file d'attente, remplissez ce champ.

Mot de passe
Mot de passe correspondant.

3.1.2.1 On-Demand Mail Relay (ODMR)

La meilleure méthode de transmission (mise en file d'attente/retrait de la file d'attente) actuellement disponible pour héberger votre courrier est ODMR. Plus performante qu'ETRN, en partie parce qu'elle requiert une authentification avant le retrait du courrier de la file d'attente, elle utilise une commande ESMTP nommée ATRN, avec laquelle le client n'a pas besoin d'une adresse IP statique puisqu'elle inverse immédiatement le flux de données entre le client et le serveur, et envoie les messages sans nécessiter de nouvelle connexion (contrairement à ETRN).

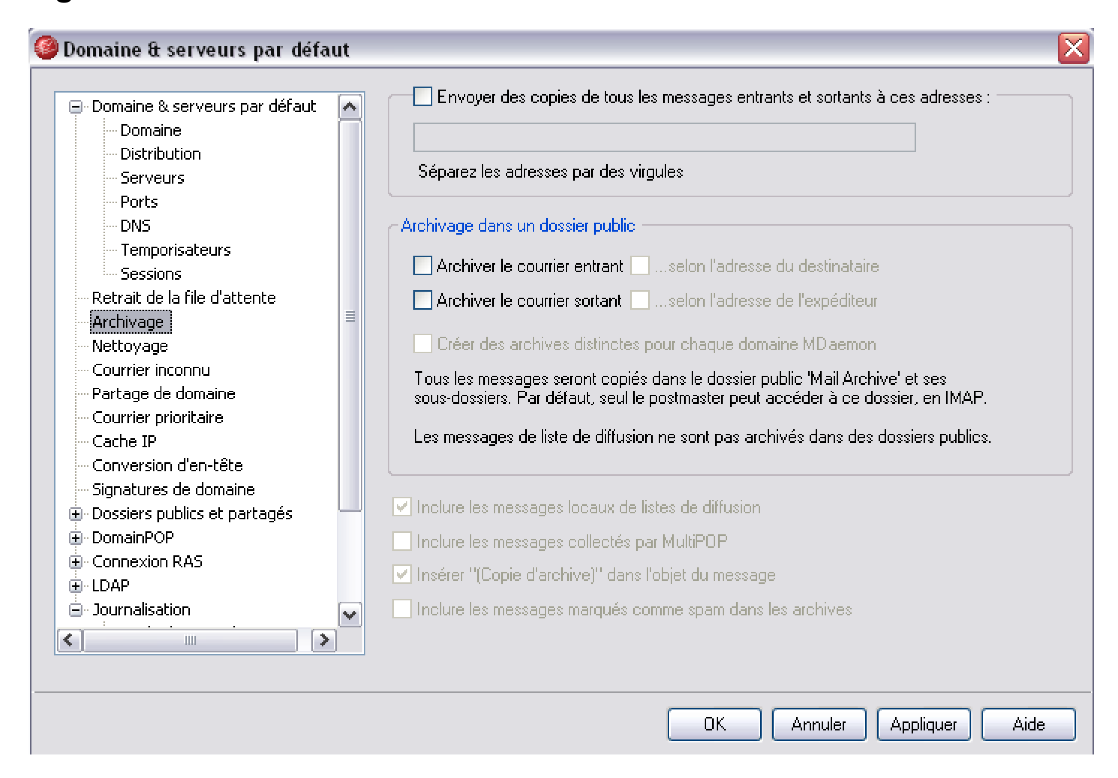
Coté client, MDaemon est totalement compatible avec ODMR, grâce à l'utilisation de la commande ATRN et des options d'authentification de l'onglet Retrait de la file d'attente 50. Il l'est également coté serveur, à l'aide des fonctionnalités de Passerelle de domaine 414.

Certains serveurs de messagerie ne supportent pas ODMR. Par conséquent, veuillez vous renseigner auprès de votre fournisseur avant d'utiliser cette méthode.

Voir également :

Passerelles » Retrait de la file d'attente 414

3.1.3 Archivage



Envoyer des copies de tous les messages entrants et sortants à ces adresses :
Saisissez une ou plusieurs adresses auxquelles vous voulez envoyer les messages d’archive, en les séparant par des virgules. Vous pouvez spécifier des adresses locales, distantes ou des alias d’adresses.

Archivage dans un dossier public

Archiver le courrier entrant
Cochez cette case pour enregistrer une copie de tous les messages entrants dans le dossier public Mail Archive. Par défaut, seul le postmaster peut accéder à ce dossier via IMAP. Pour modifier ces droits d’accès ou les élargir, utilisez la liste de contrôle d'accès 70 des dossiers publics.

...selon l’adresse du destinataire
Cochez cette case si vous voulez que l’archive du courrier entrant soit classée en fonction de l’adresse électronique du destinataire.

Archiver le courrier sortant
Cochez cette case pour enregistrer une copie de tous les messages sortants dans le

dossier public Mail Archive. Par défaut, seul le postmaster peut accéder à ce dossier via IMAP. Pour modifier ces droits d’accès ou les élargir, utilisez la liste de contrôle d'accès 70 des dossiers publics.

...selon l’adresse de l’expéditeur
Cochez cette case si vous voulez que l’archive du courrier sortant soit classée en fonction de l’adresse électronique de l’expéditeur.

Créer des archives distinctes pour chaque domaine MDaemon
Sélectionnez cette option si vous souhaitez définir une archive séparée pour chaque domaine.

Paramètres d'archivage

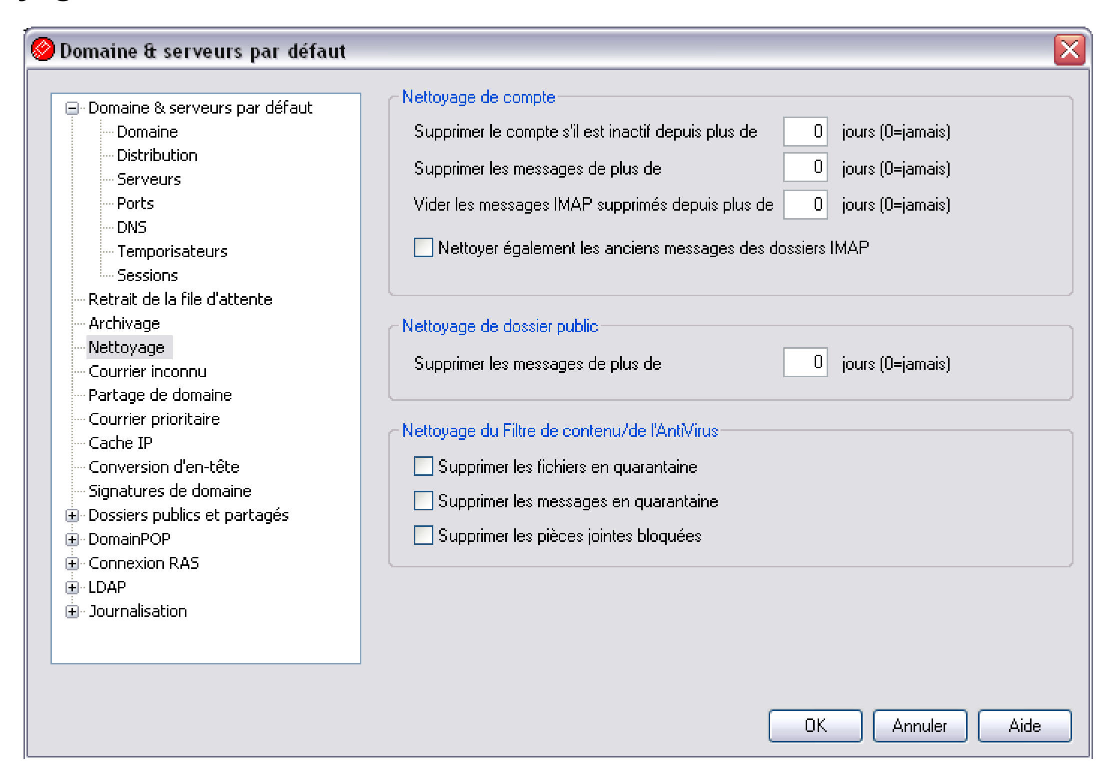
Inclure les messages locaux de liste de diffusion
Activez cette option si vous souhaitez que les messages de liste de diffusion soient inclus dans l’archive.

Inclure les messages collectés par MultiPOP
Activez cette option si vous souhaitez que les messages collectés avec MultiPOP 320 soient archivés.

Insérer "(Copie d'archive)" dans l'objet du message
Lorsque cette option est activée, le texte "(Copie d'archive)" est inséré dans les messages archivés.

Inclure les messages marqués comme spam dans les archives
Activez cette option si vous souhaitez archiver les messages marqués comme spams.

3.1.4 Nettoyage



Les options de la première section de cette boîte de dialogue servent à définir si les comptes inactifs ou les anciens messages d'un domaine doivent être supprimés par MDaemon. Chaque soir à minuit, MDaemon supprime tous les messages et comptes qui dépassent la limite de temps fixée. Pour configurer ces limites pour vos autres domaines, des paramètres similaires sont disponibles dans la boîte de dialogue Domaines supplémentaires. Il est également possible de configurer ces options individuellement pour chaque compte.
Les autres options sont globales et s'appliquent à tous les domaines.



Lorsque que d'anciens messages sont nettoyés, MDaemon ne les supprime pas vraiment, il les enregistre dans le dossier …\BADMSGS\[Mailbox]\ où ils peuvent être supprimés plus tard manuellement par l'administrateur ou par traitement chaque soir. **Remarque :** cela ne s'applique qu'au nettoyage des anciens messages. Lorsqu'un compte est nettoyé, il est supprimé et ses messages le sont également. Consultez le fichier `AccountPrune.txt` dans le dossier "…`MDaemon\App\`" pour en savoir plus et connaître les options en ligne de commande.

Nettoyage des comptes et anciens messages

Supprimer le compte s'il est inactif depuis plus de X jours (0 = jamais)
Indiquez le nombre de jours pendant lequel un compte de ce domaine peut rester inactif avant d'être supprimé. Si vous entrez la valeur "0" dans ce champ, les

comptes ne seront jamais supprimés même s'ils sont inactifs.

Supprimer les messages de plus de X jours (0 =jamais)
La valeur indiquée dans ce champ correspond au nombre de jours pendant lequel un message reste dans la boîte aux lettres d'un utilisateur avant d'être supprimé automatiquement par MDaemon. La valeur "0" signifie que les messages ne seront jamais supprimés en raison de leur ancienneté.

Vider les messages IMAP supprimés depuis plus de X jours (0 = jamais)
Utilisez cette option pour indiquer le nombre de jours pendant lequel le courrier IMAP marqué comme supprimé est conservé dans les dossiers de vos utilisateurs. Les messages marqués et supérieurs à ce nombre de jours sont éliminés de leur boîte aux lettres. La valeur "0" signifie que les messages marqués comme supprimés ne sont jamais effacés en raison de leur ancienneté.

Nettoyer également les anciens messages des dossiers IMAP
Cochez cette case si vous souhaitez que l'option *Supprimer les messages de plus de…* s'applique également aux messages des dossiers IMAP. Lorsque cette option est désactivée, les messages contenus dans ces dossiers ne seront pas supprimés en raison de leur ancienneté.

Nettoyage des dossiers publics

Supprimer les messages de plus de X jours (0 =jamais)
Indiquez une valeur dans ce champ si vous souhaitez que les anciens messages soient supprimés des Dossiers publics.

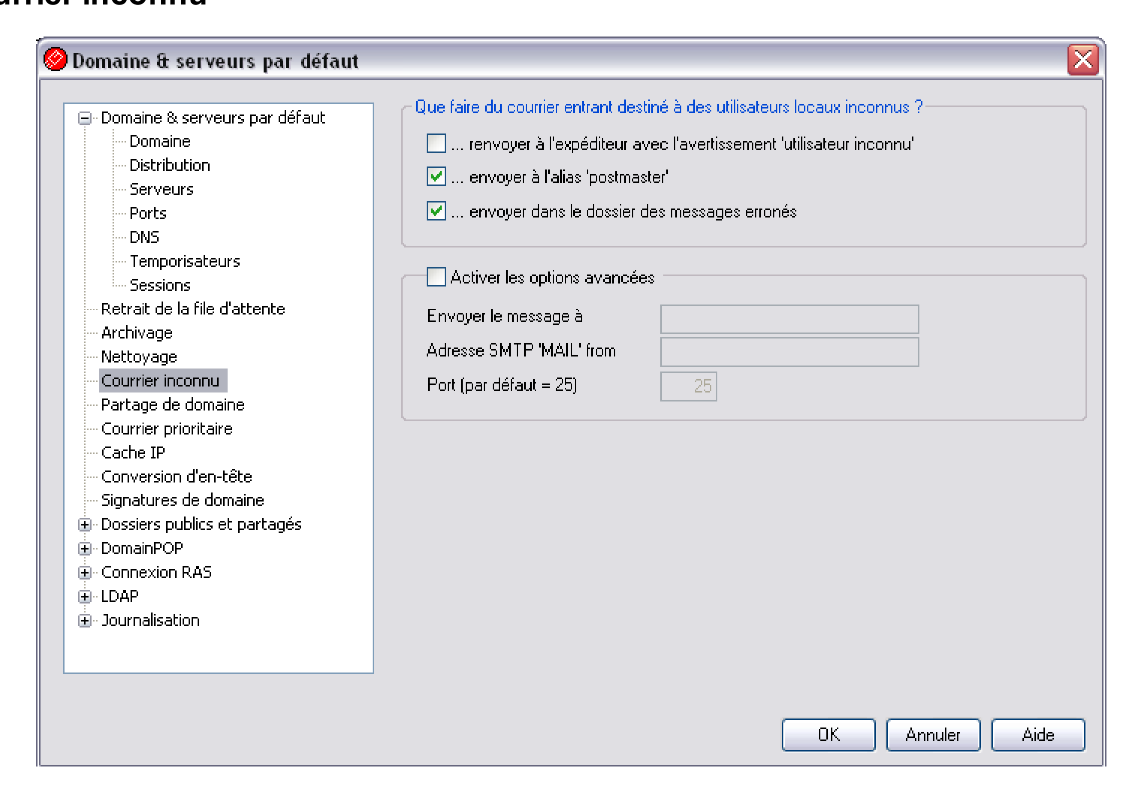
Nettoyage du Filtre de contenu/de l'antivirus

Supprimer les fichiers en quarantaine
Les fichiers mis en quarantaine sont supprimés tous les soirs.

Supprimer les messages en quarantaine
Les messages mis en quarantaine sont supprimés tous les soirs.

Supprimer les pièces jointes bloquées
Les pièces jointes filtrées sont supprimées tous les soirs.

3.1.5 Courrier inconnu



Que faire du courrier entrant destiné à des utilisateurs locaux inconnus ?

...renvoyer à l'expéditeur avec l'avertissement "utilisateur inconnu"
Lorsque cette option est activée, les messages destinées à des utilisateurs inconnus du domaine local sont renvoyés à leur expéditeur.

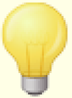
...envoyer à l'alias "postmaster"
Par défaut, les messages qui arrivent sur le serveur, et qui sont destinés à des utilisateurs locaux inconnus, sont transférés à l'utilisateur "Postmaster".

...envoyer dans le dossier des messages erronés
Par défaut, les messages qui arrivent sur le serveur et qui sont destinés à des utilisateurs locaux inconnus sont acheminés vers la file des messages erronés.

Options avancées

Activer les options avancées
Cochez cette case pour accéder aux options ci-dessous.

Envoyer le message à
L'hôte de messagerie indiqué dans ce champ recevra le courrier adressé à des utilisateurs locaux inconnus.



Lorsque vous indiquez un hôte auquel le courrier doit être transféré, copié, ou envoyé, saisissez son nom entre crochets [ ] pour ne pas effectuer de vérification MX lors de la distribution. Par exemple, si vous indiquez 'altn.com' les vérifications MX sont effectuées normalement, mais si vous indiquez '[altn.com]', seuls les enregistrements A sont vérifiés.

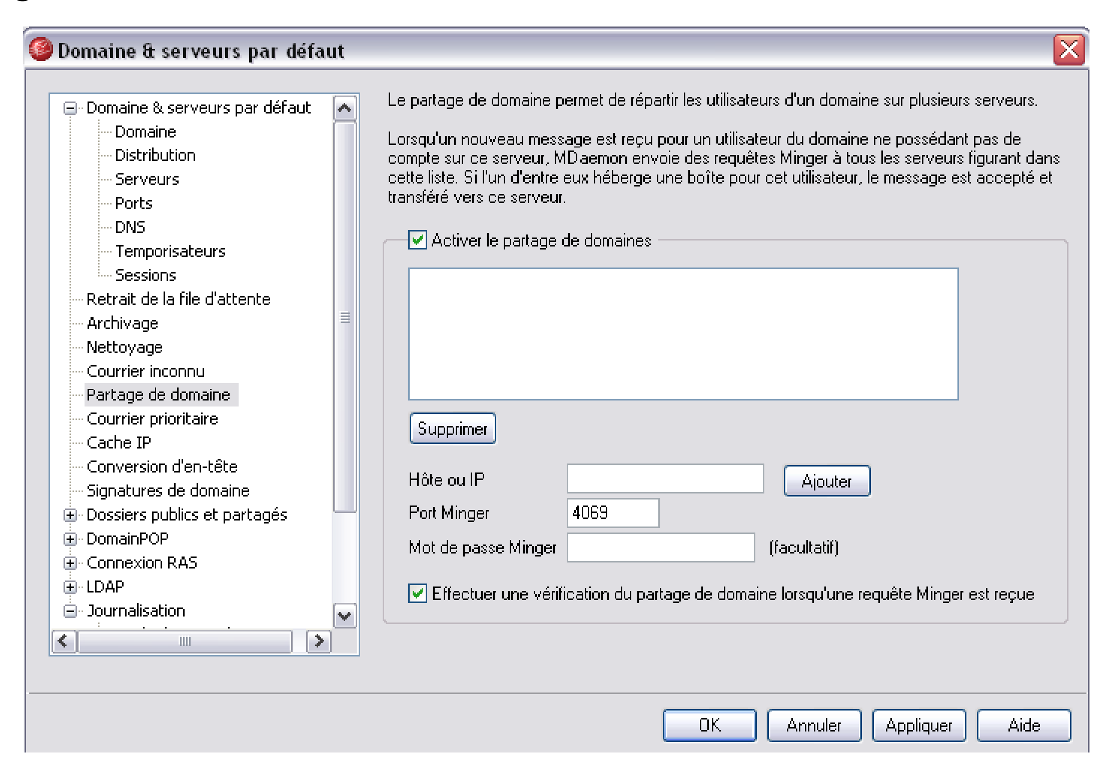
Adresse SMTP 'MAIL from"

Adresse SMTP "Mail From:" utilisée durant l'établissement d'une session avec l'hôte récepteur. Normalement, la valeur figurant dans cette portion de l'enveloppe SMTP est l'expéditeur du message. Si vous avez besoin d'une commande vide (MAIL FROM <>), indiquez alors « [trash] » dans ce champ.

Port (par défaut=25)

MDaemon envoie le courrier sur le port TCP indiqué, plutôt que sur le port SMTP sortant par défaut.

3.1.6 Partage de domaine



Cet outil permet de répartir les utilisateurs du domaine par défaut 33 et des domaines supplémentaires 103 sur plusieurs serveurs. Ainsi, il est possible d'avoir plusieurs serveurs MDaemon appartenant au même domaine, mais situés à des emplacements différents et possédant chacun des utilisateurs différents. Lorsqu'un nouveau message est reçu pour un utilisateur du domaine ne possédant pas de compte local, cet outil interroge tous les autres serveurs configurés afin de savoir lequel héberge ce compte.

Le message est alors normalement accepté et routé vers le serveur correspondant.

Par exemple, si une société possède un seul domaine (exemple.com) et des bureaux dans plusieurs villes ; avec le partage de domaine chacun de ses bureaux possède un serveur MDaemon hébergeant uniquement les comptes locaux.

Le partage de domaine est basé sur Minger369. Minger doit donc être activé et correctement configuré sur chaque serveur pour que les requêtes fonctionnent. Si une erreur se produit au cours d'une requête Minger, MDaemon renvoie une erreur temporaire "451" afin que le serveur expéditeur renouvelle sa tentative d'envoi ultérieurement. De plus, lorsqu'une adresse a été vérifiée, elle est mise en cache pendant 5 jours afin d'accélerer le traitement des prochains messages destinés à cette adresse.

Enfin, afin d'éviter qu'un même compte ne soit créé sur plusieurs serveurs, MDaemon interroge tous les serveurs du domaine avant de créer un nouveau.



L'onglet Options418 de l'Éditeur de passerelles contient une option appelée "*Les vérifications Minger déclenchent également les vérifications du Partage de domaine*". Elle permet d'interroger les hôtes du partage de domaine chaque fois qu'une passerelle effectue une vérification Minger409.

Activer le partage de domaines
Une fois cette option activée, ajoutez les hôtes supplémentaires et assurez-vous que Minger369 est correctement configuré pour la vérification des adresses.

Supprimer
Pour supprimer un hôte de la liste, sélectionnez-le et cliquez sur ce bouton.

Hôte ou IP
Nom ou adresse IP de l'hôte partageant le domaine. Si vous souhaitez utiliser un port spécifique pour l'envoi des messages SMTP à l'hôte, vous pouvez l'indiquer après deux points (ex. `mail.example.com:2525`). Attention à ne pas confondre ce port avec le port Minger ci-dessous.

Port Minger
Port utilisé par Minger pour interroger cet hôte (par défaut : 4069).

Mot de passe Minger (facultatif)
Si l'hôte exige un mot de passe, indiquez-le ici. L'utilisation de mots de passe avec Minger n'est obligatoire, mais elle est recommandée.

Ajouter
Après avoir indiqué le nom ou l'IP de l'hôte, le port et le mot de passe, cliquez sur ce bouton pour l'ajouter à la liste.

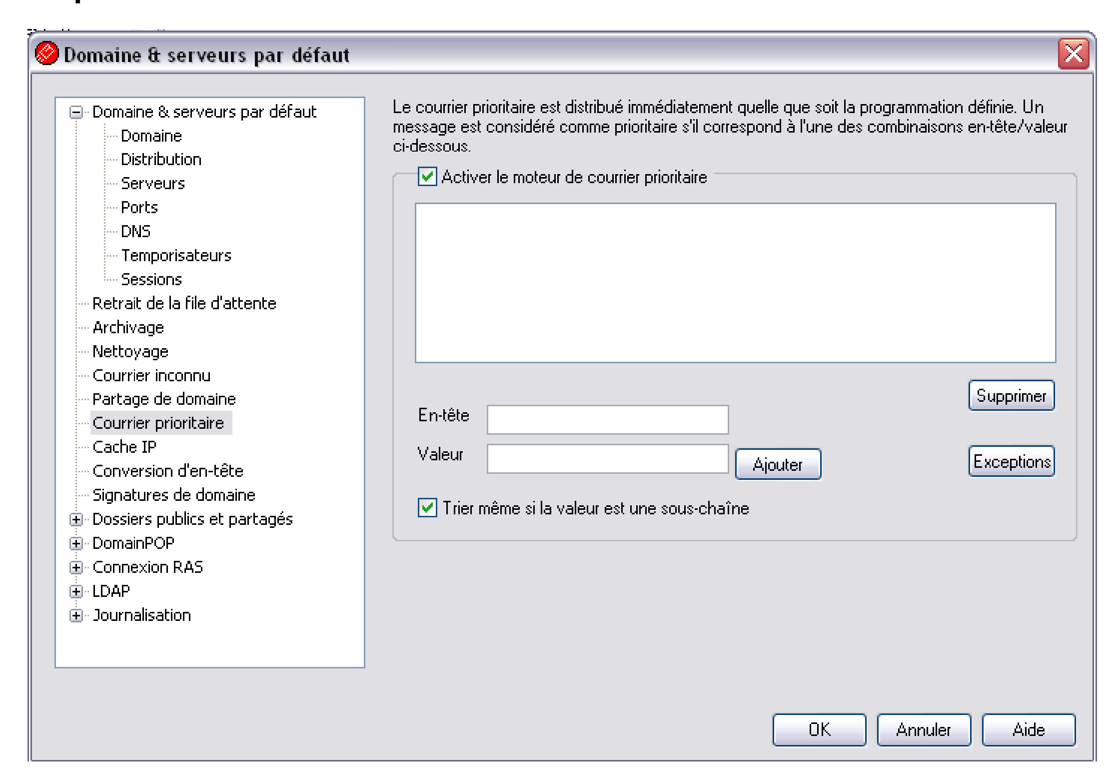
Effectuer une vérification du partage de domaine lorsqu'une requête Minger est reçue
Par défaut, le serveur Minger soumet les requêtes reçues à une vérification du partage de domaine, lorsque celui-ci est activé. Désactivez cette option si vous ne

souhaitez pas envoyer les requêtes Minger au partage de domaine.

Voir également :

[Minger](369)
[Domaine par défaut](33)
[Domaines supplémentaires](103)

3.1.7 Courrier prioritaire



Le courrier prioritaire est distribué immédiatement par MDaemon sans tenir compte des intervalles de traitement du courrier programmés. Lorsqu'un nouveau message arrive, MDaemon inspecte ses en-têtes et recherche les combinaisons en-tête/valeur que vous avez indiquées dans cette boîte de dialogue. S'il les trouve, il considèrera que le message est prioritaire et tentera de le distribuer immédiatement.

Moteur de courrier prioritaire

Activer le moteur de courrier prioritaire
Cochez cette case pour activer cette fonctionnalité.

En-tête
Indiquez un en-tête (sans les deux-points qui le terminent).

Valeur
Valeur devant être contenue dans l'en-tête ci-dessus pour que le message soit considéré comme prioritaire.

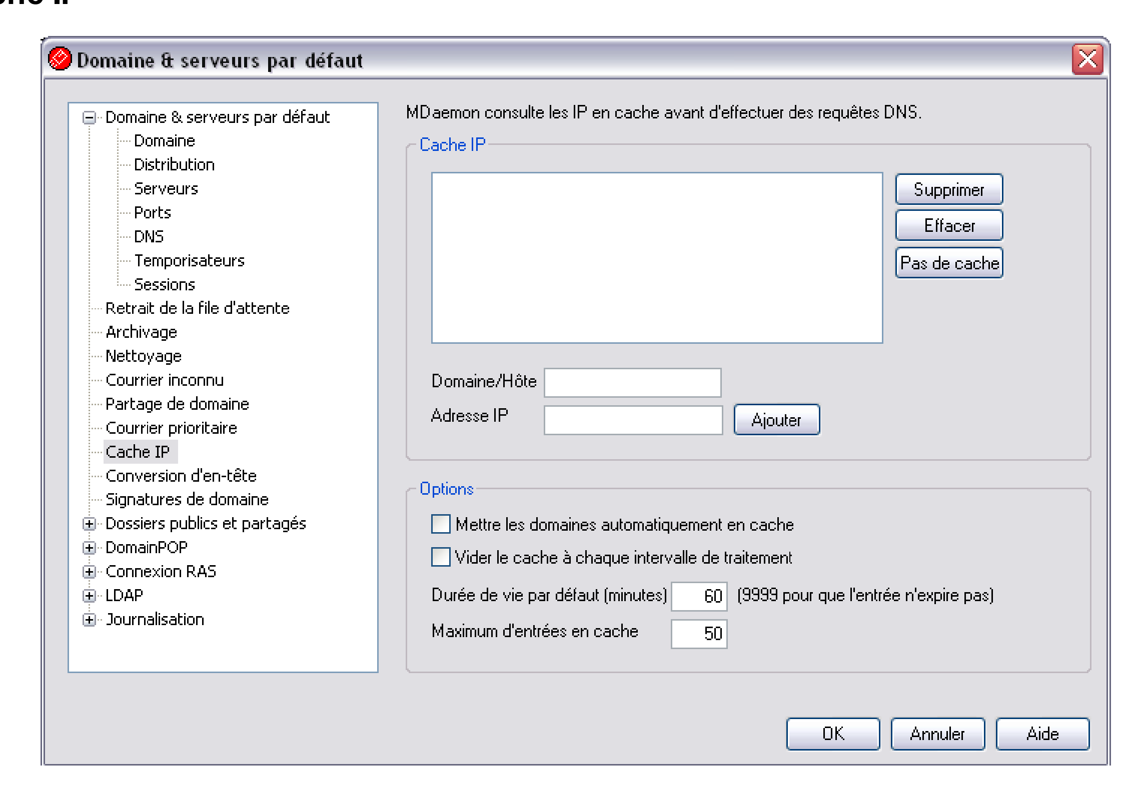
Trier même si la valeur est une sous-chaîne
Cette option permet d'activer le courrier prioritaire même si la valeur indiquée est simplement une partie (ou sous-chaîne) de l'en-tête. Par exemple, vous pouvez créer une entrée avec l'en-tête "`To`" et la valeur "directeur". Dans ce cas, il suffit que cet en-tête contienne "`directeur@undomaine`" pour que le message soit considéré comme prioritaire. Lorsque cette option n'est pas activée, le contenu de l'en-tête doit correspondre exactement à la valeur indiquée.

Ajouter
Après avoir rempli les champs ci-dessus, cliquez sur ce bouton pour ajouter une nouvelle entrée à la liste.

Supprimer
Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Exceptions
Cliquez sur ce bouton si vous souhaitez définir des combinaisons en-tête/valeur auxquelles le courrier prioritaire ne s'applique pas.

3.1.8 Cache IP



Afin d'accélerer la distribution des messages et de diminuer le temps de traitement du courrier, MDaemon met en cache les adresses IP de tous les hôtes auxquels il se connecte. Ces IP sont stockées et le cache est vérifié chaque fois que MDaemon exige une résolution DNS sur un nom de domaine. Si le nom de domaine nécessitant une résolution est trouvé dans le cache IP, la résolution DNS n'a pas lieu, ce qui permet de réduire considérablement le temps de traitement. Les paramètres de cette fenêtre permettent d'agir sur les paramètres de fonctionnement du cache. Vous pouvez également ajouter et supprimer manuellement des entrées et définir la taille maximale du cache.

Cache IP

Domaine / Hôte
Nom de domaine ou d'hôte à ajouter au cache IP.

IP
Adresse IP du domaine ou de l'hôte à ajouter au cache.

Ajouter
Après avoir rempli les deux champs ci-dessus, cliquez sur ce bouton pour ajouter l'entrée à la liste.

Supprimer
Pour supprimer une IP en cache de la liste, sélectionnez-la et cliquez sur ce bouton.

Effacer
Ce bouton supprime toutes les entrées du cache.

Pas de cache
Cliquez sur ce bouton si vous souhaitez définir une liste de noms de domaines et/ou adresses IP à ne jamais mettre en cache.

Options

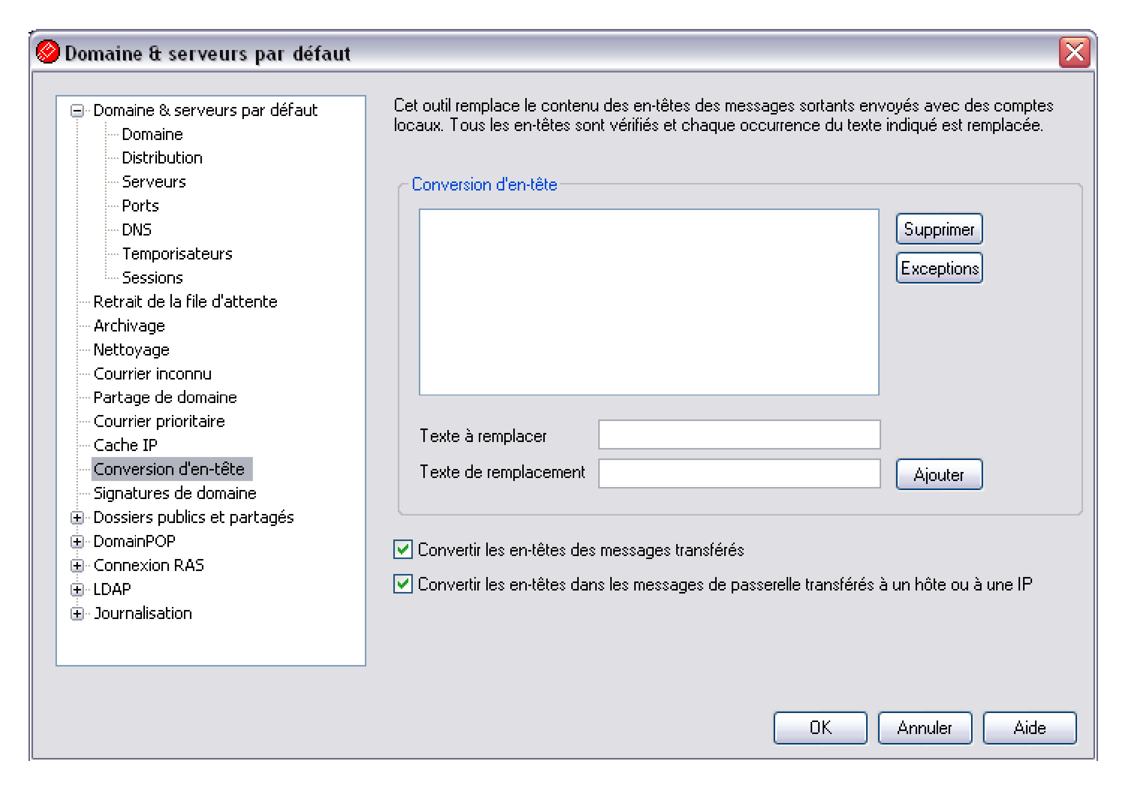
Mettre les domaines automatiquement en cache
Ce paramètre contrôle le moteur interne de mise en cache automatique de MDaemon. Si vous voulez que MDaemon mette automatiquement les domaines en cache, activez cette option. Si vous voulez constituer vous-même votre cache IP, décochez cette case.

Vider le cache à chaque intervalle de traitement
Si vous sélectionnez cette option, tout le contenu du cache sera vidé au démarrage de chaque session de messagerie. Cela permet d'actualiser le cache à chaque intervalle de traitement.

Durée de vie par défaut (minutes)
Il s'agit de la valeur par défaut en minutes pendant laquelle une entrée reste dans le cache IP. Une fois ce laps de temps écoulé, MDaemon supprime l'entrée du cache. Si vous souhaitez définir une entrée permanente dans le cache IP, fixez alors la Durée de vie par défaut sur 9999.

Maximum d’entrées en cache
Cette option limite la taille du cache. Une fois la limite atteinte, l'enregistrement d'une nouvelle entrée supprime la plus ancienne.

3.1.9 Conversion d'en-tête



Cette fonctionnalité permet de remplacer un fragment de texte trouvé dans un en-tête par une nouvelle valeur, à chaque fois qu’un message de votre domaine est envoyé à l'extérieur. Il suffit d'indiquer le texte que vous voulez rechercher ainsi que sa valeur de remplacement. MDaemon recherche alors dans tous les en-têtes du message et effectue les remplacements. Vous pouvez également indiquer des en-têtes que MDaemon ne doit pas modifier (comme par exemple les en-têtes "Subject:" ou "Received:") en cliquant sur le bouton "Exceptions" de cette boîte de dialogue.

Cette fonctionnalité est nécessaire dans certaines configurations de MDaemon lorsque par exemple le nom de domaine local est fictif ou différent de celui qui doit apparaître dans le courrier sortant. Dans ce cas, la conversion d’en-tête peut être utilisée pour transformer chaque occurrence de "@domainelocal.com" en "@DomaineDistant.com".

Conversion d'en-tête

Supprimer
Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Exceptions
Cliquez sur ce bouton pour ouvrir la boîte de dialogue Exceptions63. Elle permet de

définir des en-têtes auxquels la conversion ne s'applique pas.

Texte à remplacer
Saisissez le texte que vous souhaitez remplacer lorsqu'il est trouvé dans les en-têtes d'un message sortant.

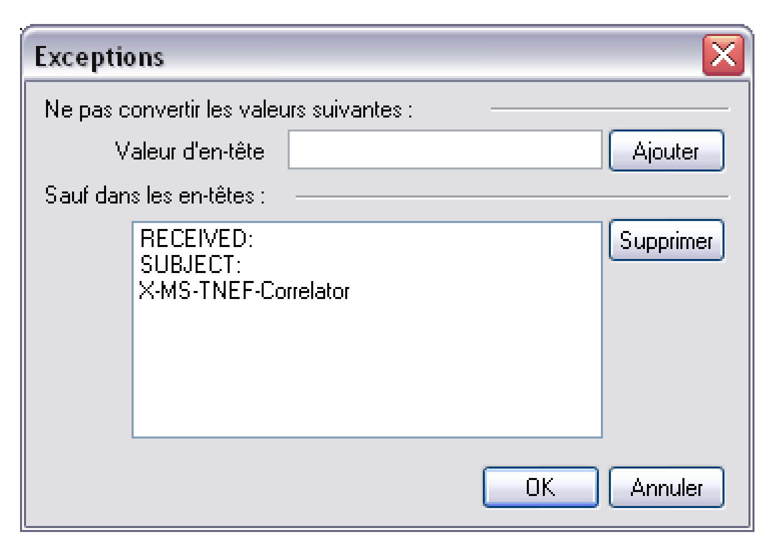
Texte de remplacement
Ce texte remplacera celui qui se trouve dans le champ *Texte à remplacer*.

Ajouter
Après avoir rempli les deux champs ci-dessus, cliquez sur ce bouton pour ajouter une nouvelle entrée à la liste.

Convertir les en-têtes des messages transférés
Activez cette option pour que les conversions d'en-têtes s'appliquent également aux messages transférés automatiquement d'un domaine local vers un domaine non local.

Convertir les en-têtes dans les messages de passerelle transférés à un hôte ou à une IP
Activez cette option si vous voulez que les en-têtes soient convertis dans les messages de passerelle transférés. Voir l'onglet Transfert 413 de l'Éditeur de passerelle pour en savoir plus.

3.1.9.1 Exceptions de la conversion d'en-têtes



Ne pas convertir les valeurs suivantes

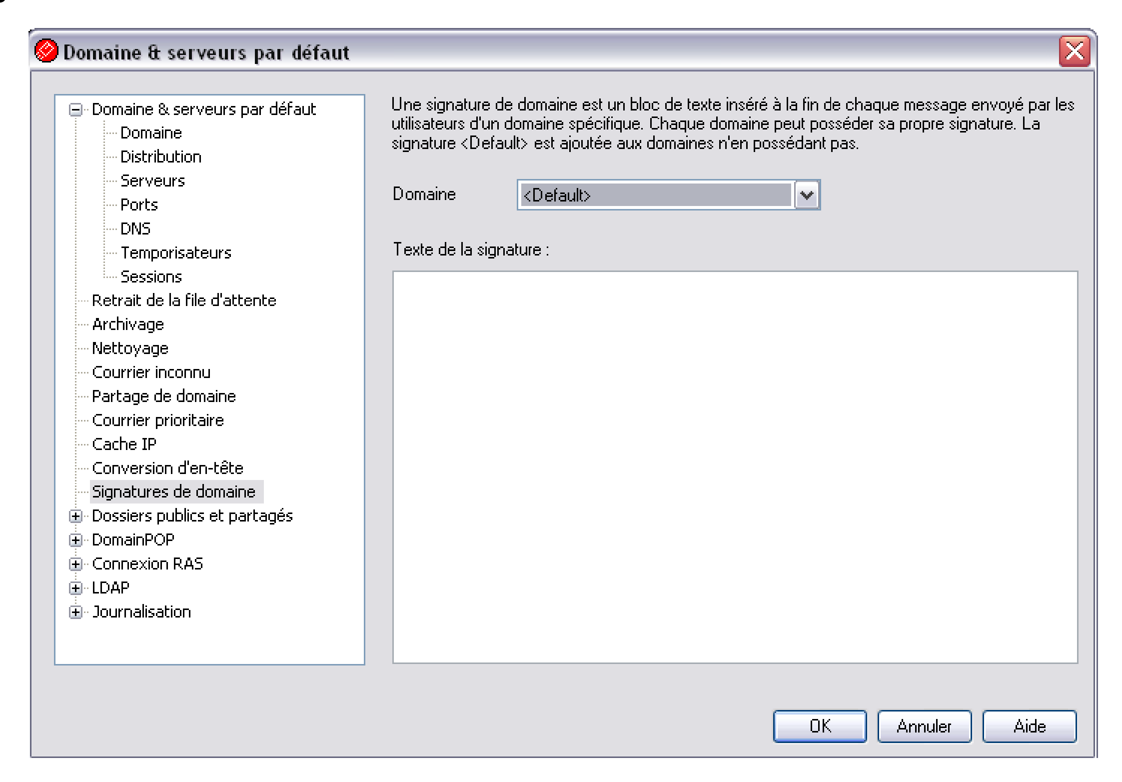
Valeur d'en-tête
Si vous ne souhaitez pas que la conversion s'applique à un en-tête spécifique, saisissez son nom dans ce champ, puis cliquez sur le bouton Ajouter.

Sauf dans les en-têtes

Liste des en-têtes auxquels la conversion ne s'applique pas.

Supprimer
Pour supprimer un en-tête de la liste, sélectionnez-le et cliquez sur ce bouton.

3.1.10 Signatures de domaine



Cette boîte de dialogue permet de créer facilement un texte, par défaut ou par domaine, qui servira de signature pour vos messages. Si vous avez défini une signature par défaut, elle sera ajoutée à tous les messages envoyés par des utilisateurs locaux (sauf si une signature est définie pour un domaine spécifique). Les signatures des domaines sont prioritaires sur la signature par défaut. Les signatures figurent toujours après le texte du message. Cependant, si une liste de diffusion utilise un pied de page, la signature est affichée avant le pied de page.

Vous pouvez également définir une signature 327 pour chaque utilisateur. Elle s'affiche juste avant la signature du domaine.

3.1.11 Dossiers publics & partagés

MDaemon propose un sytème de partage de dossiers publics et dossiers IMAP utilisateurs. Les dossiers publics sont des dossiers supplémentaires qui n'appartiennent à aucun compte en particulier mais qui peuvent être mis à disposition de plusieurs utilisateurs IMAP. Les dossiers utilisateurs sont des dossiers IMAP qui appartiennent à des comptes MDaemon individuels. Chaque dossier partagé doit être associé à une liste d'utilisateurs MDaemon, et seuls les membres de cette liste y ont accès via WorldClient

ou un client de messagerie IMAP.

Lorsque des utilisateurs IMAP accèdent à leur liste de dossiers personnels, les dossiers publics et utilisateurs partagés auxquels ils ont accès seront également affichés. Ainsi, certains dossiers de messagerie peuvent être partagés par plusieurs utilisateurs mais chacun devra fournir ses identifiants de connexion personnels. De plus, pouvoir accéder à un dossier ne signifie pas nécessairement avoir un droit en lecture/écriture ou un accès administrateur sur celui-ci. Des droits d'accès spécifiques peuvent être accordés à des utilisateurs individuels, ce qui vous permet de leur attribuer différents niveaux d'accès. Par exemple, vous pouvez n'autoriser que certains utilisateurs à supprimer des messages.

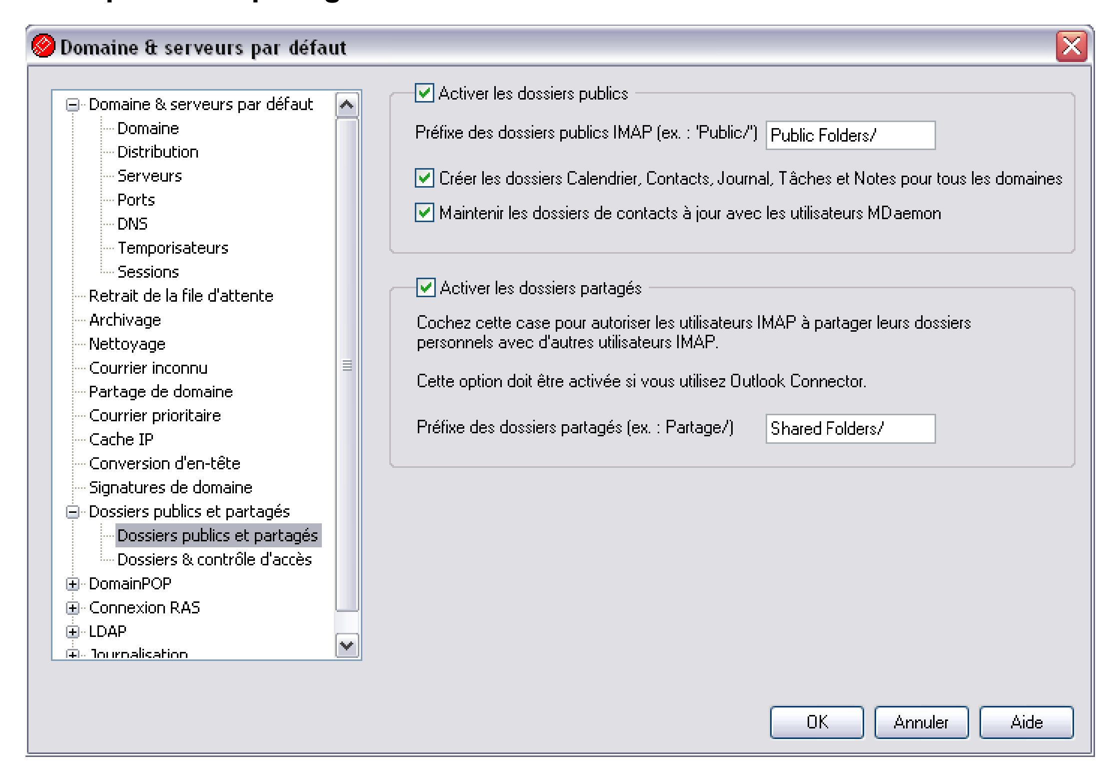
Lorsqu'un dossier IMAP public ou utilisateur est créé, vous pouvez utiliser le Filtre de contenu pour définir des critères qui entraîneront le déplacement de certains messages vers ce dossier. Par exemple, il peut être utile d'élaborer une règle 180 selon laquelle les messages contenant support@mydomain.com dans l'en-tête À: seront déplacés vers le dossier public Support. Pour acheminer des messages spécifiques vers les dossiers partagés, les utilisateurs disposent de filtres IMAP 307. De plus, vous pouvez associer un compte spécifique à un dossier partagé afin que les messages destinés à cette adresse soient acheminés automatiquement vers ce dossier partagé. Toutefois, seuls les utilisateurs qui ont une autorisation "d'envoi" vers ce dossier pourront faire parvenir des messages à cette adresse.

L'éditeur de liste de diffusion contient également un onglet Dossiers Publics qui permet de configurer un dossier public utilisable avec une liste en particulier. Si vous activez cette fonctionnalité, une copie de chaque message de la liste est placée dans le dossier public indiqué. Tous les dossiers publics sont stockés dans le répertoire \Public Folders\ de MDaemon.

Voir également :

Dossiers publics et partagés 66
Liste des dossiers 68
Contrôle d'accès 70
Éditeur de compte » Dossiers partagés 322

3.1.11.1 Dossiers publics et partagés



Dossiers publics

Activer les dossiers publics
Sélectionnez cette option si vous souhaitez autoriser les utilisateurs IMAP à accéder aux dossiers publics. Les utilisateurs autorisés ainsi que le niveau d'accès accordé sont indiqués sous chaque fichier dans la liste des dossiers 68. Décochez cette case si vous souhaitez que les dossiers publics soient masqués.

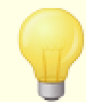
Préfixe des dossiers publics IMAP (ex. : 'Public/')
Il est possible d'ajouter au début du nom des dossiers publics une chaîne pouvant comporter jusqu'à 20 caractères, telle que "#" ou "Public-". Cela permet aux utilisateurs de distinguer facilement les dossiers publics des dossiers privés dans leur logiciel de messagerie. Saisissez dans cette zone de texte les caractères que vous souhaitez utiliser pour indiquer qu'il s'agit de dossiers publics.

Créer les dossiers Calendrier, Contacts, Journal, Tâches et Notes pour tous les domaines
Cochez cette case si vous souhaitez que chaque domaine contienne ces dossiers. Ils sont créés automatiquement lorsque vous ajoutez un domaine supplémentaire 104 à MDaemon.

Maintenir les dossiers de contact à jour avec les utilisateurs MDaemon
Lorsque cette option est activée, MDaemon synchronise le contenu du dossier de contacts avec la liste des comtpes.

Dossiers partagés

Activer les dossiers partagés
Autorise les utilisateurs IMAP à partager l'accès à leurs dossiers IMAP. Les utilisateurs autorisés ainsi que le niveau d'accès accordé sont indiqués sous chaque dossier dans l'onglet Dossiers partagés 322 de l'éditeur de compte. En décochant cette case, vous empêchez les utilisateurs de partager l'accès à leurs dossiers et l'onglet Dossiers Partagés n'apparaît pas.



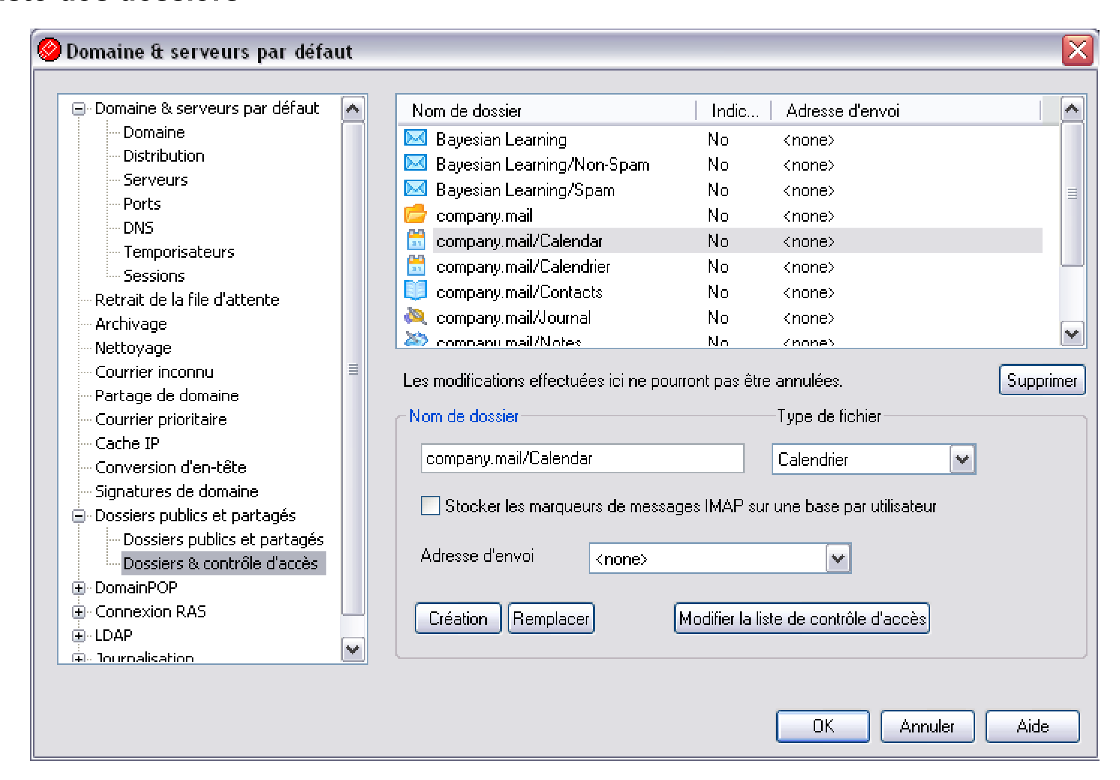
Si vous utilisez Outlook Connector, cette option n'est pas disponible. Vous ne pourrez pas la décocher car le partage des dossiers est nécessaire au bon fonctionnement d'Outlook Connector.

Préfixe des dossiers partagés (ex. : 'Partage/')
Il est possible d'ajouter au début du nom des dossiers partagés une chaîne pouvant comporter jusqu'à 20 caractères, telle que "#" ou "Partage/". Cela permet aux utilisateurs de distinguer facilement les dossiers partagés des dossiers privés dans leur logiciel de messagerie. Saisissez dans cette zone de texte les caractères que vous souhaitez utiliser pour indiquer qu'il s'agit de dossiers partagés.

Voir également :

Liste des dossiers 68
Liste de contrôle d'accès 70
Editeur de compte » Dossiers partagés 322

3.1.11.2 Liste des dossiers



Pour atteindre cette fenêtre, cliquez sur "Configuration » Domaine/serveurs par défaut » Dossiers publics et partagés » Dossiers et contrôle d'accès".

Dossiers IMAP

Cette fenêtre affiche les dossiers IMAP que vous avez créés, les drois d'accès accordés ainsi que les éventuelles Adresses d'envoi associées.

Supprimer
Pour supprimer un dossier IMAP de la liste, sélectionnez-le et cliquez sur ce bouton.

Nouveau dossier IMAP

Nom de dossier
Pour ajouter un dossier à la liste, indiquez son nom dans ce champ, sélectionnez le type de fichier et l'adresse d'envoi puis cliquez sur Créer. Si vous voulez que le nouveau dossier soit un sous-dossier de l'un des dossiers de cette liste, préfixez alors le nom du nouveau dossier avec le nom du dossier parent et un slash. Par exemple, si le dossier parent s'appelle "Mon dossier" et le nouveau "Mon deuxième dossier", le nom du nouveau dossier est "Mon dossier/Mon nouveau dossier".

Type de fichier
Sélectionnez un type dans le menu déroulant : Courrier, Contacts, Calendrier, etc.

Stocker les marqueurs de messages IMAP sur une base par utilisateur
Activez cette option si vous souhaitez que les marqueurs des messages contenus

dans ces dossiers (lu, non lu, répondu, transféré, etc.) soient définis par utilisateur et non globalement. Ainsi, si un utilisateur a ouvert un message, il le voit marqué comme lu ; alors qu'un utilisateur qui ne l'a pas ouvert le voit marqué comme non lu. Si cette option est désactivée, tous les utilisateurs voient le même marqueur. Dans ce cas, il suffit qu'un utilisateur ouvre un message pour que tous les autres le voient marqué comme "lu".

Adresse d'envoi
Utilisez cette liste déroulante pour associer un compte spécifique à un dossier partagé afin que les messages destinés à cette Adresse d'envoi soient automatiquement acheminés vers le dossier partagé indiqué. Toutefois, seuls les utilisateurs ayant le droit "Envoi" sur ce dossier pourront envoyer du courrier vers cette adresse.

Créer
Après avoir indiqué un nom de dossier et configuré les autres paramètres, cliquez sur ce bouton pour ajouter le dossier à la liste.

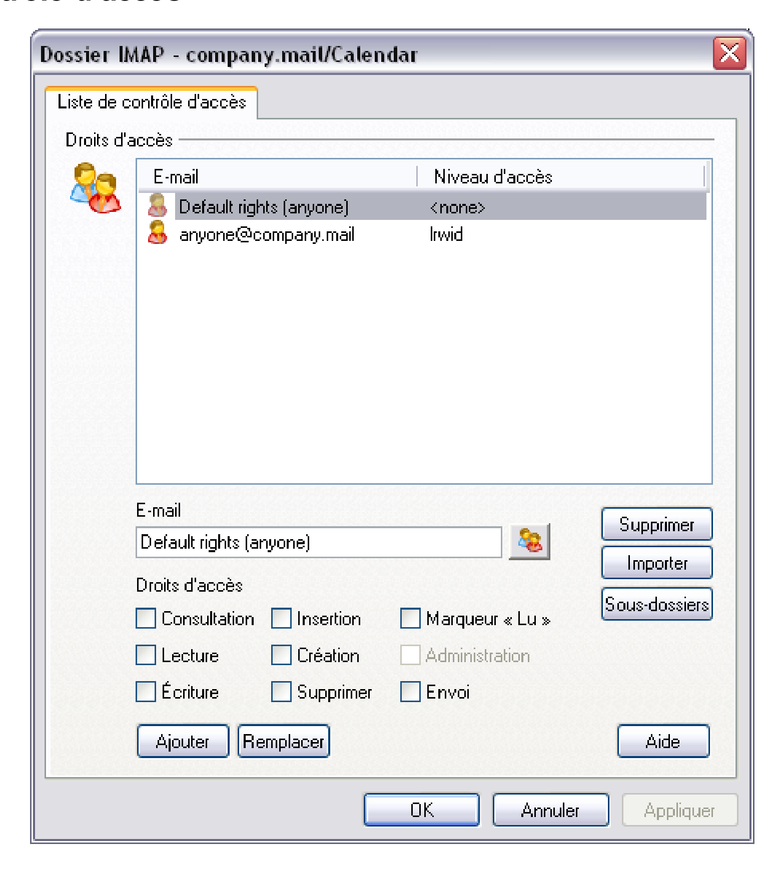
Remplacer
Si vous souhaitez modifier une des entrées des dossiers publics, cliquez sur ce bouton, effectuez les modifications voulues au Nom de dossier ou à un autre paramètre, puis cliquez sur Remplacer.

Modifier la liste de contrôle d'accès
Pour modifier les droits d'accès à un dossier, sélectionnez-le et cliquez sur ce bouton.

Voir également :

Liste de contrôle d'accès 70
Dossiers publics & partagés 66
Editeur de compte » Dossiers partagés 322

3.1.11.2.1 Liste de contrôle d'accès



Droits d'accès

Cette boîte de dialogue permet d'indiquer les comptes utilisateurs ou groupes auxquels vous souhaitez accorder l'accès à un dossier partagé, ainsi que les droits d'accès pour chacun d'eux. Pour y accéder, cliquez sur "Configuration » Domaine/serveurs par défaut » Dossiers publics et partagés » Dossiers & contrôle d'accès". Chaque entrée présente l'adresse électronique du compte et une abréviation d'une lettre indiquant le niveau d'accès pour chaque droit accordé à l'utilisateur.

E-mail

Saisissez une adresse e-mail ou cliquez sur l'icône pour accorder les droits d'accès à un compte ou un groupe. Après avoir indiqué le compte ou groupe de votre choix, choisissez les droits d'accès puis cliquez sur le bouton Ajouter.

Supprimer

Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Importer

Cliquez sur ce bouton pour ajouter les membres d'une liste de diffusion existante à la liste des utilisateurs ayant des droits d'accès. Choisissez les droits d'accès que vous souhaitez accorder à ces utilisateurs, cliquez sur Importer, puis double-cliquez sur la liste souhaitée. Tous ses membres seront ajoutés à la liste avec les droits d'accès que vous avez définis.

Sous-dossiers
Sélectionnez un compte ou groupe et cliquez sur ce bouton si vous souhaitez appliquer les droits à tous les sous-dossiers du dossier sélectionné. Si le compte ou groupe possède déjà des droits pour l'un des sous-dossiers, ils seront remplacés par ceux indiqués ici.

Droits d'accès

Cochez les correspondant aux droits que vous souhaitez accorder, puis cliquez sur *Ajouter* ou sur *Remplacer* pour les entrées existantes.

Vous pouvez accorder les droits d'accès suivants :

Consultation (l) – l'utilisateur peut voir ce dossier dans sa liste personnelle de dossiers IMAP.

Lecture (r) – l'utilisateur peut ouvrir ce dossier et lire son contenu.

Écriture (w) – l'utilisateur peut modifier les marqueurs sur les messages de ce dossier.

Insertion (i) – l'utilisateur peut ajouter et copier des messages dans ce dossier.

Création (c) – l'utilisateur peut créer des sous-dossiers dans ce dossier.

Suppression (d) – l'utilisateur peut supprimer des messages de ce dossier.

Marqueur "lu" (s) – l'utilisateur peut modifier le statut lu/non lu des messages de ce dossier.

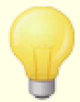
Administration (a) – l'utilisateur peut administrer la liste de contrôle d'accès pour ce dossier.

Envoi (p) – l'utilisateur peut envoyer du courrier directement vers ce dossier (si le dossier le permet).

Ajouter
Après avoir sélectionné l'adresse e-mail ou le groupe ainsi que les droits accordés, cliquez sur ce bouton pour ajouter le compte ou le groupe à la liste.

Remplacer
Pour modifier les droits d'accès d'une entrée existante, sélectionnez-la dans la liste, effectuez les modifications voulues dans les droits d'accès, puis cliquez sur Remplacer.

Aide
Cliquez sur Aide pour afficher une liste des droits d'accès ainsi que leur définition.



Les droits d'accès sont contrôlés grâce au support des listes de contrôle d'accès (ACL). Elles constituent une extension du protocole IMAP4 qui permet de créer une liste d'accès pour chacun de vos dossiers de messages IMAP, et accorde ainsi des droits d'accès à vos dossiers à d'autres utilisateurs qui

> possèdent également des comptes sur votre serveur de messagerie. Si votre client de messagerie n'est pas compatible avec les ACL, vous pouvez toujours définir ces autorisations à l'aide des commandes de cette boîte de dialogue.
>
> Pour obtenir des informations complètes sur les ACL, consultez : http://www.rfc-editor.org/rfc/rfc2086.txt.

Voir également :

Dossiers publics et partagés 66
Liste des dossiers 68

3.1.12 DomainPOP

Cette fonctionnalité utilise le protocole POP pour télécharger la totalité du courrier trouvé dans une boîte aux lettres POP de votre FAI associée au nom de connexion indiqué. Une fois collectés, les messages sont analysés selon les paramètres fournis dans cette boîte de dialogue, puis placés dans les boîtes des utilisateurs ou dans la file d'attente du courrier distant. MDaemon pourra ainsi les distribuer, comme si ces messages étaient arrivés sur le serveur à l'aide de transactions SMTP classiques.

Il est important de savoir que les messages stockés dans des boîtes aux lettres POP, et récupérés à l'aide du protocole POP, ne contiennent pas certaines informations de routage importantes (appelées parfois "enveloppe du message"), qui sont habituellement présentes lorsque les messages sont distribués à l'aide du protocole SMTP. Sans ces informations de routage, MDaemon est obligé de "lire" le courrier et d'examiner les en-têtes pour essayer de déterminer son destinataire. Avec SMTP, le contenu du message n'est pas déterminant, puisque le protocole indique lui-même au serveur, durant la transaction de courrier, le destinataire visé du message.

Afin de permettre une extraction et une distribution POP efficace du courrier électronique, MDaemon utilise plusieurs options performantes pour le traitement des en-têtes. Lorsque MDaemon télécharge un message depuis une source POP distante, il analyse immédiatement tous ses principaux en-têtes et établit un ensemble de destinataires potentiels. Toutes les adresses électroniques trouvées dans les en-têtes que MDaemon analyse, sont incluses dans cette collecte.

Une fois cette opération terminée, la collecte de destinataires effectuée par MDaemon, est partagée en deux ensembles (local et distant). De plus, toutes les adresses analysées et placées dans cette collecte de destinataires potentiels, sont traitées par le convertisseur d'alias 347 d'adresses avant d'être réparties. Chaque membre de l'ensemble local (les adresses avec un domaine qui correspond soit au domaine par défaut soit à l'un des domaines supplémentaires de MDaemon) recevra une copie du courrier concerné. L'ensemble distant est contrôlé par les paramètres de cette boîte de dialogue.

Veillez à empêcher la duplication de messages ou la distribution de courrier en boucle.

Lors de la perte de l’enveloppe SMTP, il est courant de rencontrer des problèmes avec du courrier provenant de listes de diffusion. Généralement, le corps des messages distribués par une liste de diffusion ne contient aucune référence aux adresses des destinataires. Au contraire, le moteur de liste insère simplement le nom de la liste de diffusion dans le champ A:. Cela pose un problème : si le champ A: contient le nom de la liste de diffusion, il est possible que MDaemon télécharge ce message, analyse le champ A: (qui va correspondre au nom de la liste de diffusion), puis renvoie le message à la même liste. Tour à tour, une copie du même message sera distribuée à la boîte aux lettres POP à partir de laquelle MDaemon a téléchargé le message d’origine—renouvelant ainsi la totalité du cycle. Pour faire face à de tels problèmes, les administrateurs de messagerie doivent veiller à utiliser les outils et les paramètres fournis par MDaemon, qui leur permettent de supprimer le courrier provenant de listes de diffusion, ou à lui donner un alias, de sorte que le courrier soit distribué aux destinataires locaux appropriés. Vous pouvez également utiliser les règles de routage ou le Filtre de contenu pour distribuer le courrier aux bons destinataires.

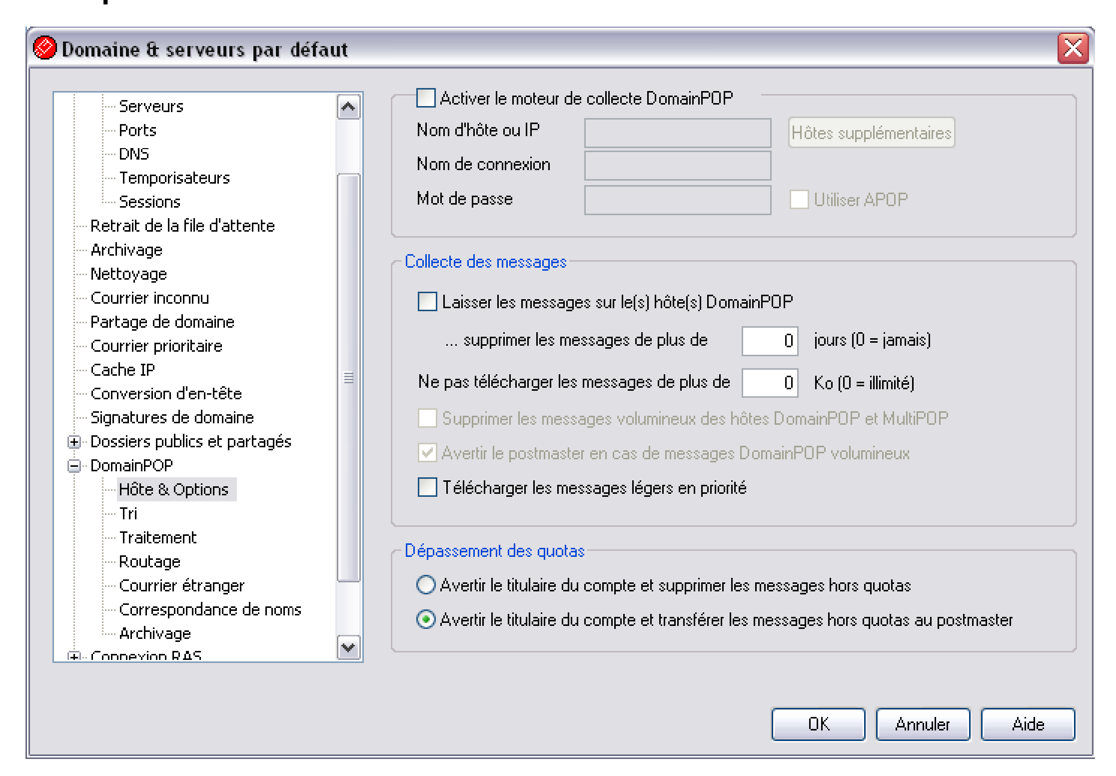
La duplication involontaire de messages pose des problèmes supplémentaires lorsque l’on utilise ce type de collecte. Le courrier distribué à la boîte aux lettres POP du FAI, à l’aide de SMTP, peut facilement générer des duplications non souhaitées de messages, une fois qu’ils ont été collectés à l’aide de DomainPOP. Par exemple, supposons qu’un message soit envoyé à un utilisateur de votre domaine et qu’une copie carbone soit envoyée à un autre utilisateur du même domaine. Dans ce cas, le protocole SMTP entraîne la distribution de deux copies du même message à la boîte aux lettres de votre FAI—une pour chaque destinataire, celui du champ A: et celui du champ CC:. MDaemon collectera ces deux fichiers de message identiques et analysera chacune de leurs adresses. Les deux destinataires recevront alors un message en double. Pour se protéger de la duplication, MDaemon utilise une commande où vous pouvez indiquer un en-tête qu’il utilisera pour vérifier la présence de copies en double. Le champ Message-ID est idéal pour cela. Dans l’exemple ci-dessus, les deux messages identiques contiendront ainsi la même valeur dans le champ Message-ID. MDaemon peut utiliser cette valeur pour identifier et supprimer le second message lors du téléchargement, avant que ces informations d’adresse ne soient analysées.

Enfin, MDaemon détecte le nombre de passages ou de "sauts" qu’un message a effectué au cours de sa distribution. À chaque fois qu’un serveur de messagerie SMTP traite un message, il le "marque" avec un en-tête "Received". MDaemon compte tous ces en-têtes lorsqu’il rencontre un message pour la première fois. Si le nombre total de serveurs qui ont marqué le courrier dépasse une valeur indiquée, il est probable que le message soit pris dans une boucle de distribution. Il doit alors être sorti du flux de courrier et déplacé vers le répertoire des messages erronés. Le nombre de sauts autorisés peut être configuré dans l'onglet Temporisateurs 45 de l'Éditeur du domaine principal.

Voir également :

Filtre de contenu 177
Liste de diffusion 378

3.1.12.1 Hôte & Options



Propriétés de l'hôte DomainPOP

Activer le moteur de collecte DomainPOP
Si vous sélectionnez cette option, MDaemon utilise les paramètres de cette boîte de dialogue pour collecter le courrier depuis un serveur de messagerie DomainPOP.

Nom d'hôte ou IP
Entrez dans ce champ le nom de domaine ou l'adresse IP de votre hôte DomainPOP.

Hôtes supplémentaires
Cliquez sur ce bouton pour ouvrir le fichier DpopXtra.dat, dans lequel il est possible d'indiquer des hôtes supplémentaires pour la collecte du courrier DomainPOP. Ce fichier contient des indications sur la syntaxe à utiliser.

Nom de connexion
Entrez votre nom de connexion du compte POP utilisé par DomainPOP.

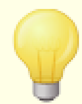
Mot de passe
Entrez le mot de passe du compte POP ou APOP dans ce champ.

Utiliser APOP
Activez cette option si vous souhaitez utiliser la commande APOP et l'authentification CRAM-MD5 lors du retrait de votre courrier. Cela permet de vous authentifier sans envoyer de mots de passe en texte clair.

Collecte des messages

Laisser une copie des messages sur l'(es) hôte(s) DomainPOP
Si vous sélectionnez cette option, MDaemon ne supprime pas les messages collectés sur l'hôte DomainPOP.

...supprimer les messages de plus de [xx] jours (0=jamais)
Indiquez la durée pendant laquelle les messages doivent être conservés sur l’hôte DomainPOP avant d’être supprimés. Indiquez 0 si vous ne souhaitez pas supprimer les anciens messages.



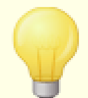
Certains hôtes peuvent limiter la durée pendant laquelle les messages sont conservés dans les boîtes.

Ne pas télécharger les messages de plus de X KO (0 = illimité)
Les messages dont la taille est supérieure ou égale à cette valeur ne sont pas téléchargés depuis votre serveur DomainPOP. Entrez "0" si vous voulez que MDaemon télécharge tous les messages quelle que soit leur taille.

Supprimer les messages volumineux des hôtes DomainPOP et MultiPOP
Si vous activez cette option MDaemon supprime les messages qui dépassent la taille indiquée. Les messages sont simplement supprimés des serveurs de messagerie DomainPOP et MultiPOP, et ne sont pas téléchargés.

Avertir le postmaster en cas de messages DomainPOP volumineux
MDaemon envoie un avertissement au postmaster lorsqu’il trouve un message volumineux dans la boîte aux lettres DomainPOP.

Télécharger les messages légers en priorité
Activez cette option si vous voulez que le téléchargement des messages se fasse par taille, du plus petit au plus volumineux.



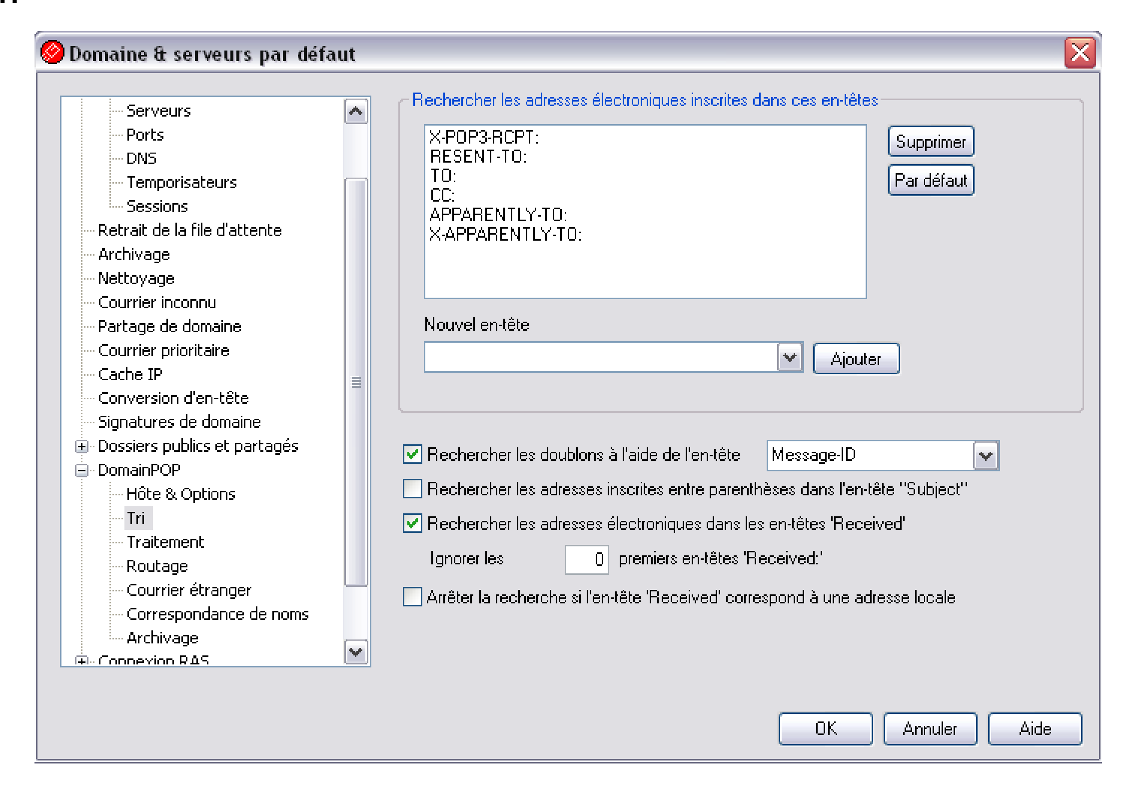
Cette option récupère les petits messages plus rapidement mais nécessite des capacités de tri et de traitement interne plus importantes.

Dépassement des quotas

Avertir le titulaire du compte et supprimer les messages hors quota
Lorsque vous choisissez cette option et qu’un message est collecté pour un compte qui est hors quota (défini dans l’onglet Quotas 317 de l’éditeur de compte), MDaemon supprime ce message et signale à l’utilisateur que son compte dépasse sa limite.

Avertir le titulaire du compte et transférer les messages hors quota au postmaster
Lorsque vous choisissez cette option et qu’un message est collecté pour un compte qui est hors quota, MDaemon transfère ce message au postmaster et signale à l’utilisateur que son compte dépasse sa limite.

3.1.12.2 Tri



Rechercher les adresses électroniques inscrites dans ces en-têtes

Liste des en-têtes analysés par MDaemon afin d'extraire les adresses.

Supprimer

Pour supprimer un en-tête de la liste, sélectionnez-le et cliquez sur ce bouton.

Par défaut

Cliquez sur ce bouton pour rétablir la liste d'en-têtes par défaut. En général, les en-têtes par défaut suffisent pour extraire toutes les adresses d’un message.

Nouvel en-tête

Entrez le nouvel en-tête que vous souhaitez ajouter à la liste.

Ajouter

Cliquez sur ce bouton pour ajouter à la liste l’en-tête figurant dans le champ Nouvel en-tête ci-dessus.

Rechercher les doublons à l'aide de l'en-tête

Si vous sélectionnez cette option, MDaemon retient la valeur de l’en-tête indiqué et ne traite pas les messages supplémentaires collectés au cours du même cycle de

courrier qui contiennent une valeur identique. Par défaut : Message-ID.

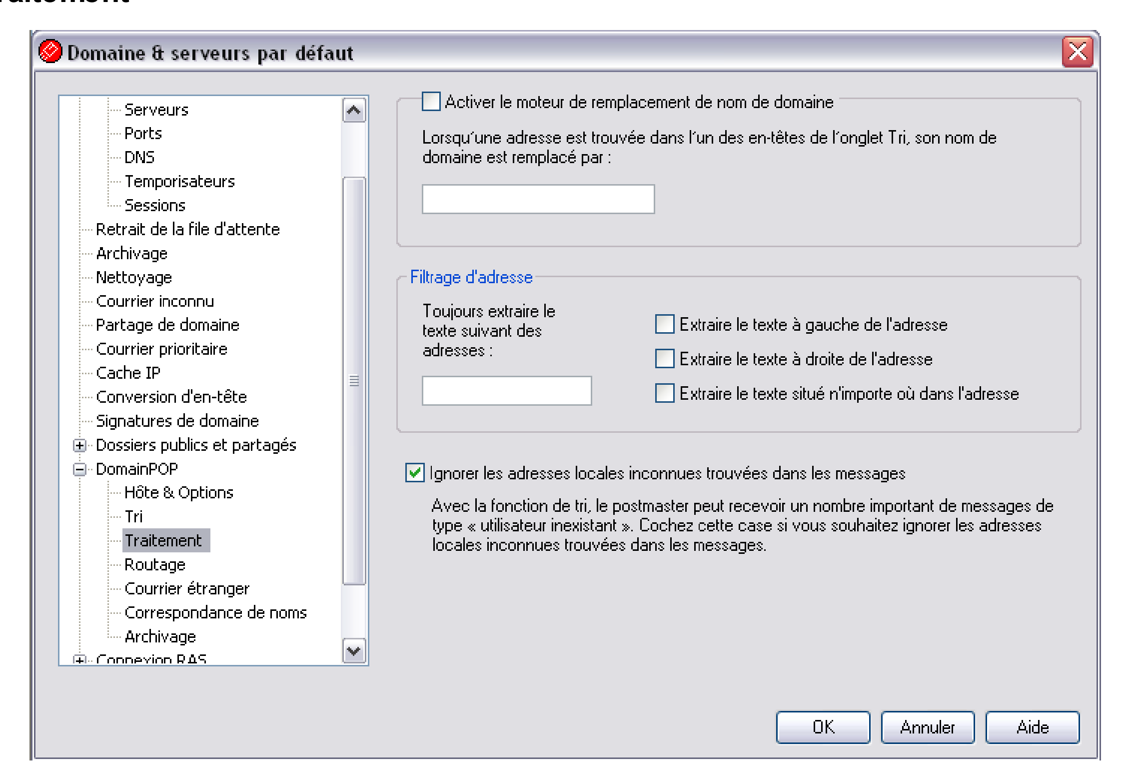
Rechercher les adresses inscrites entre parenthèses dans l'en-tête "Subject"
Lorsque cette option est sélectionnée et que MDaemon trouve une adresse entre parenthèses dans l'en-tête "Subject" d'un message, celle-ci est ajoutée à la liste des destinataires, tout comme les autres adresses obtenues.

Rechercher les adresses électroniques dans les en-têtes "Received"
Il est possible de stocker les informations du destinataire, qui ne se trouvent en général que dans l'en-tête "Received" des messages. Cela permet aux analyseurs syntaxiques de message de récupérer l'adresse actuelle du destinataire en inspectant seulement cet en-tête. Cochez cette option si vous souhaitez que MDaemon analyse tous les en-têtes "Received" des messages électroniques afin de déterminer si les adresses sont valides.

Ignorer les X premiers en-têtes "Received"
Ce champ permet d'entrer le nombre d'en-têtes "Received" que MDaemon ignore avant de commencer l'analyse.

Arrêter la recherche si l'en-tête "Received" correspond à une adresse locale
Si, au cours de l'analyse d'un en-tête "Received", MDaemon détecte une adresse locale valide, les analyses suivantes sont alors arrêtées, et MDaemon ne recherche pas d'autres adresses de distribution potentielles dans le message concerné.

3.1.12.3 Traitement



Remplacement de nom de domaine

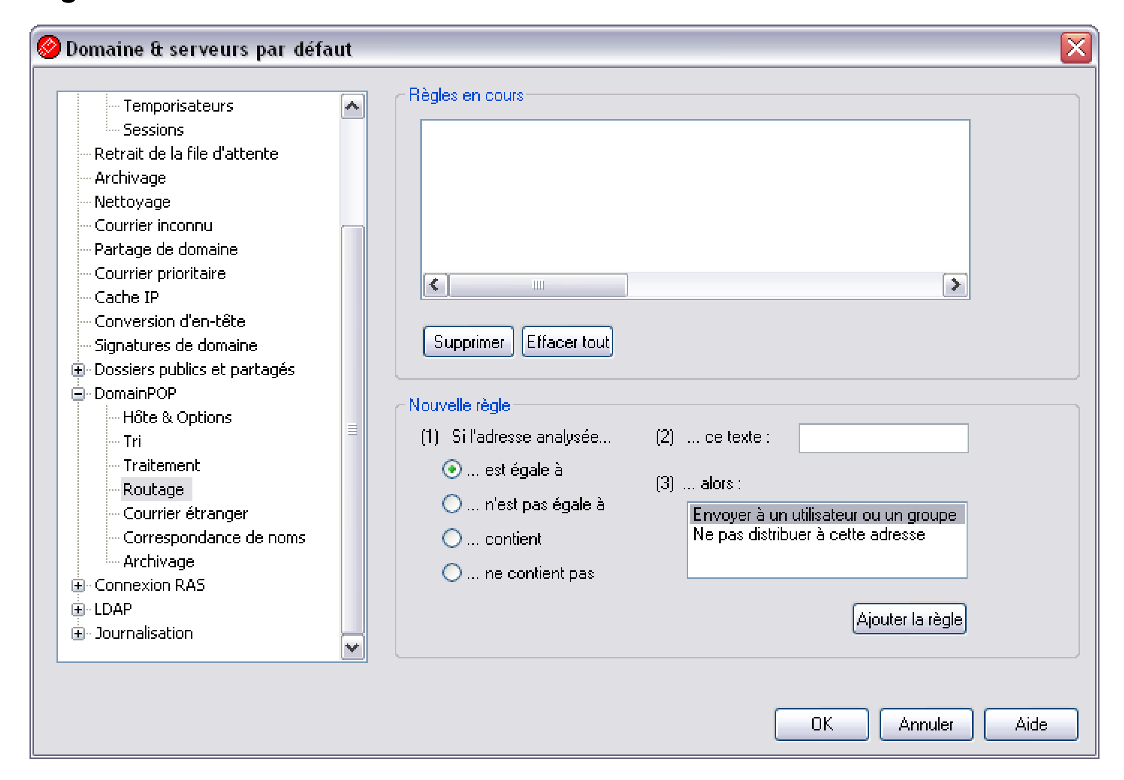
Activer le moteur de remplacement de nom de domaine
Cette option réduit le nombre d'alias de domaine de votre site. Lorsqu'un message est téléchargé, *tous* les noms de domaines de *toutes* les adresses analysées sont remplacés par celui indiqué dans le champ au-dessous.

Filtrage d'adresse

Toujours extraire le texte suivant des adresses :
Certains FAI insèrent, à droite ou à gauche de l'adresse d'un message, une ligne indiquant le destinataire ainsi que des informations de routage. Ce marquage serait idéal pour filtrer les adresses des destinataires s'il n'impliquait pas une utilisation massive d'alias de compte. C'est pourquoi vous pouvez simplement entrer une valeur dans la zone de texte et MDaemon procédera à son extraction dans chaque adresse analysée.

Ignorer les adresses locales inconnues trouvées dans les messages
Comme son nom l'indique, la fonctionnalité de Remplacement de nom de domaine remplace le nom de domaine des adresses analysées par le nom spécifié. Certaines adresses ne disposant pas de compte sur votre site peuvent être créées. Seulement, comme le nom de domaine doit correspondre à votre domaine par défaut, MDaemon considère que ces adresses locales sont inconnues, et envoie le message « Utilisateur inconnu » au postmaster. Cocher cette case évite l'envoi de ce message.

3.1.12.4 Routage



Règles en cours

Liste de toutes les règles que vous avez créées et qui sont appliquées à vos messages.

Supprimer
Pour supprimer une règle de la liste, sélectionnez-la et cliquez sur ce bouton.

Effacer tout
Cliquez sur ce bouton pour supprimer toutes les règles.

Nouvelle règle

(1) Si l'adresse analysée...

Est égale à, n’est pas égale à, contient, ne contient pas
Il s’agit du type de comparaison faite entre une adresse et la règle de routage. MDaemon recherche dans chaque adresse le texte contenu dans le champ "ce texte", puis agit en fonction de l'option sélectionnée ici.

(2) ...ce texte :
Saisissez le texte que MDaemon doit rechercher lorsqu’il analyse les adresses.

(3) ...alors :
Actions pouvant être effectuées si le résultat de la règle est positif :

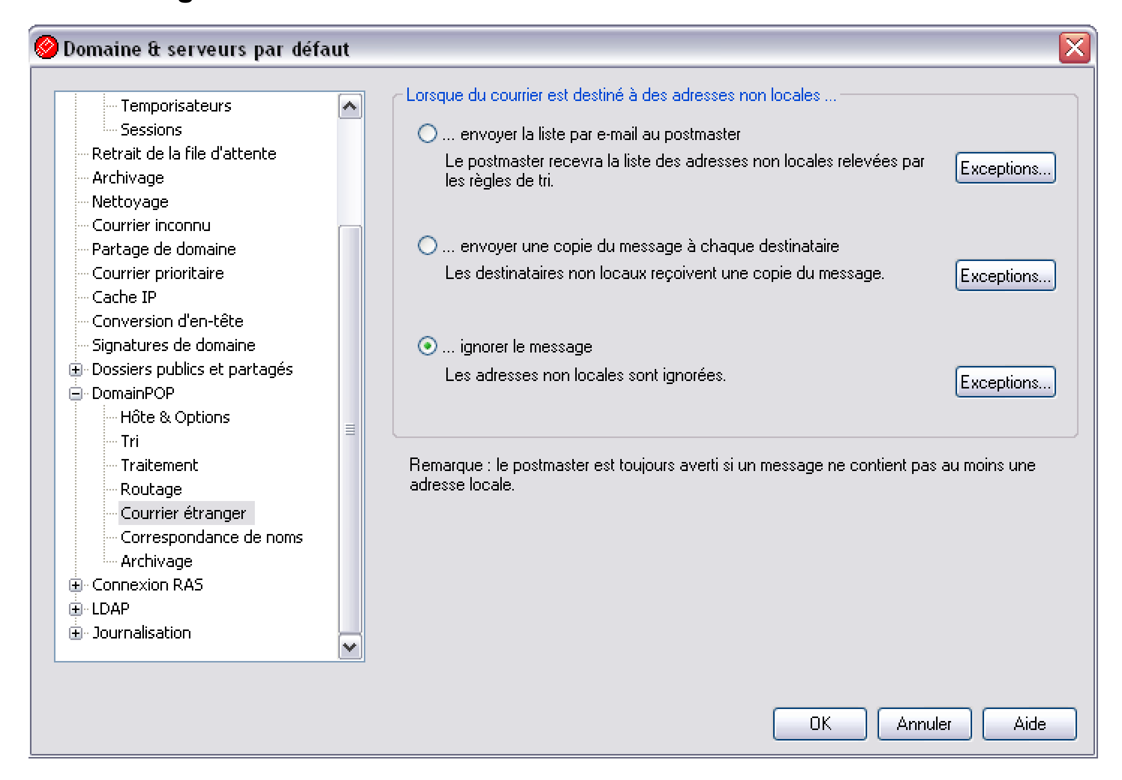
Ne pas distribuer à cette adresse - En sélectionnant cette règle, les messages ne

sont pas distribués à l'adresse indiquée.

Envoyer à un utilisateur ou un groupe - En sélectionnant cette action, une boîte de dialogue s'affiche afin d'indiquer une liste d'adresses électroniques qui doivent recevoir une copie du message traité.

Ajouter la règle
Après avoir configuré tous les paramètres, cliquez sur ce bouton pour ajouter la nouvelle règle à la liste.

3.1.12.5 Courrier étranger

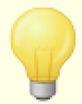


Lorsque du courrier est destiné à des adresse non locales...

...envoyer la liste par e-mail au postmaster
Si cette option est sélectionnée, MDaemon envoie une seule copie du message au postmaster ainsi que la liste des adresses non locales que le moteur de tri a extraites en se fondant sur les en-têtes et les règles de tri sélectionnés.

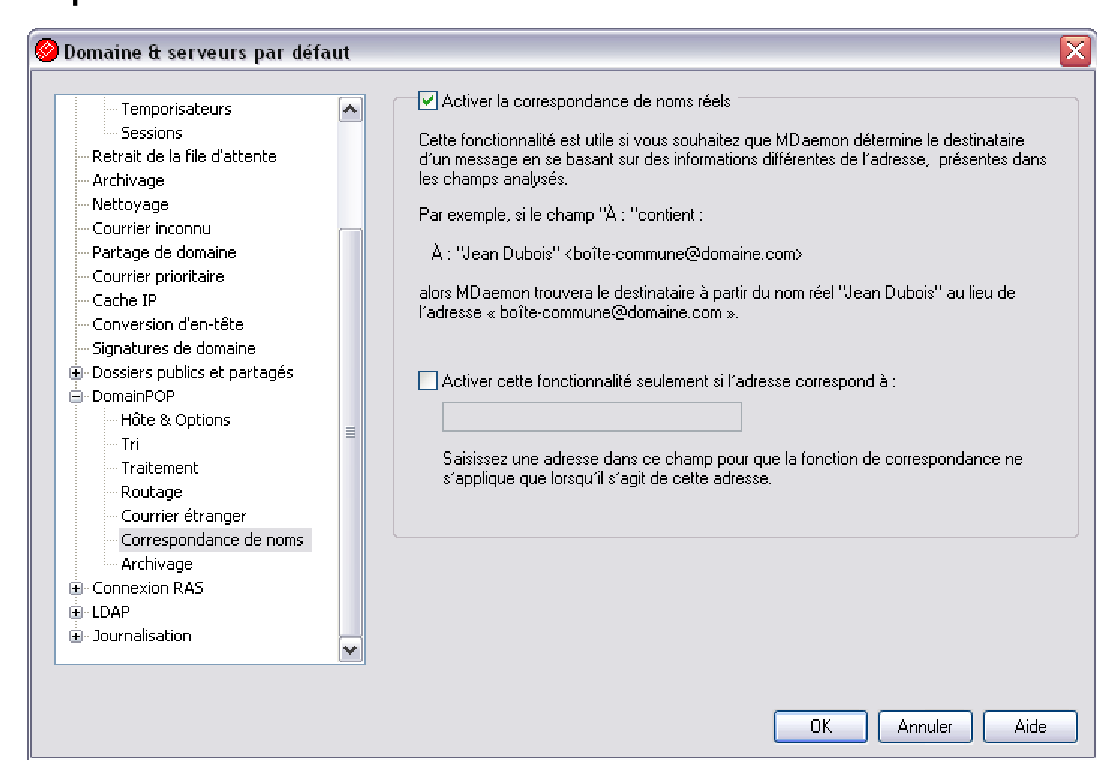
...envoyer une copie du message à chaque destinataire
Si cette option est sélectionnée, MDaemon distribue une copie du courrier aux destinataires non locaux qu'il trouve dans les en-têtes analysés.

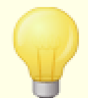
...ignorer le message
Si cette option est sélectionnée, MDaemon supprime toutes les adresses non locales de la liste des destinataires.



Les boutons *Exceptions...* permettent de définir des adresses auxquelles l'option correspondante ne s'applique pas.

3.1.12.6 Correspondance de noms





La correspondance de noms n'est active qu'avec le moteur de collecte du courrier DomainPOP. Si vous souhaitez utiliser cette fonctionnalité, assurez-vous que DomainPOP est activé.

Moteur de correspondance de noms réels

Activer la correspondance de noms réels
Cette fonctionnalité permet à MDaemon de déterminer les destinataires d'un message collecté avec DomainPOP en fonction de la portion de texte qu'il contient (en général, le nom réel d'une personne) et non de l'adresse électronique.

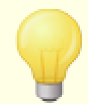
Par exemple, un en-tête TO peut être sous la forme :

```
TO: "Jean Dubois" <mailbox@exemple.com>
```

ou

```
TO: Jean Dubois <mailbox@exemple.com>
```

La correspondance de nom ignore la portion de l'adresse "mailbox@exemple.com". À la place, elle extrait la portion « Jean Dubois » et tente de vérifier s'il s'agit d'un utilisateur de MDaemon. Si une correspondance est trouvée avec le champ nom réel d'un compte, l'adresse électronique locale de ce compte est utilisée pour la distribution. Dans le cas contraire, MDaemon distribue le message normalement à l'adresse analysée dans les données (ici :mailbox@example.com).

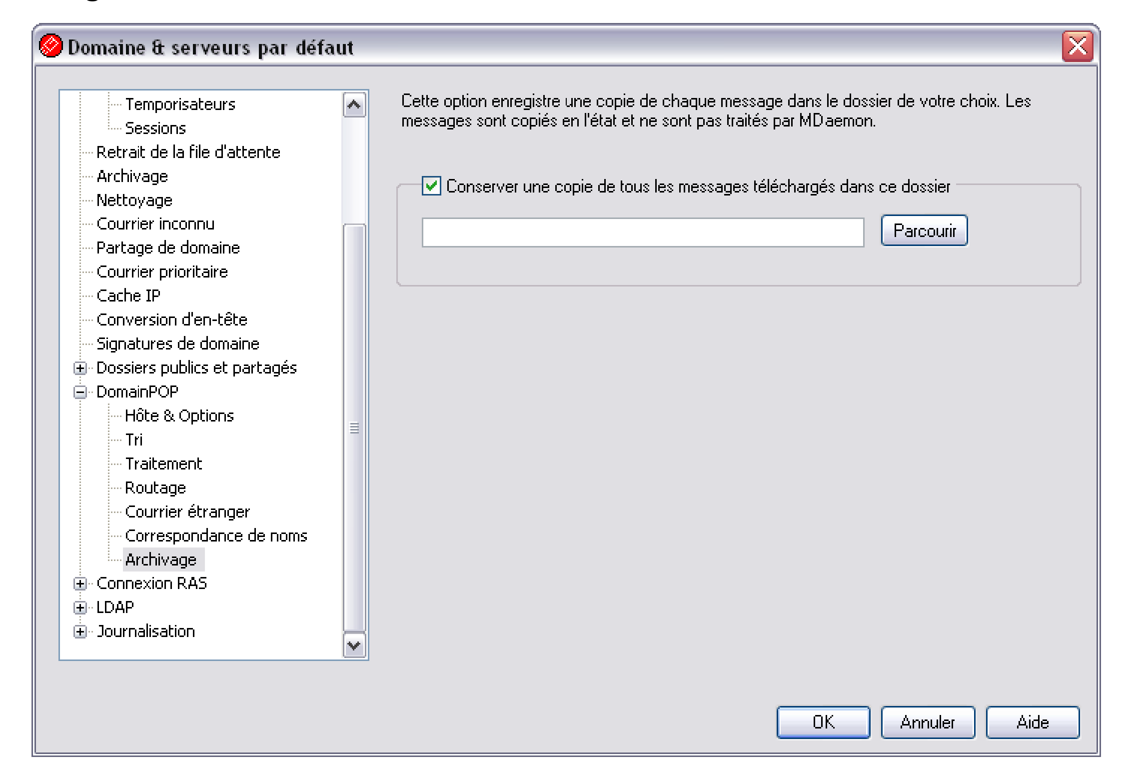


Le texte qui correspond au nom réel de l'adresse doit contenir une virgule, un point-virgule ou deux-points.

Activer cette fonctionnalité seulement si l'adresse correspond à :
Cette option permet d'exiger qu'une adresse spécifique soit présente dans les données extraites pour que la correspondance de noms fonctionne. Par exemple, vous pouvez entrer une adresse du type "mailbox@exemple.com" pour que seules les adresses correspondant à cette valeur soient traitées par la correspondance de noms.

Dans ce cas "**`TO: 'Jean Dubois' <mailbox@exemple.com>`**" sera traité par la correspondance de noms, mais "**`TO: 'Jean Dubois' <Jean@example.com>`** sera ignoré.

3.1.12.7 Archivage



Archivage

Conserver une copie de tous les messages téléchargés dans ce dossier
Il s'agit d'une mesure de sécurité qui vous protège contre la perte de courrier à cause d'une erreur d'analyse ou d'autres erreurs pouvant survenir lors du téléchargement d'un grand nombre de messages. Cette option enregistre une copie de chaque message dans le dossier indiqué. Les messages sont copiés en l'état et ne sont pas traités par MDaemon.

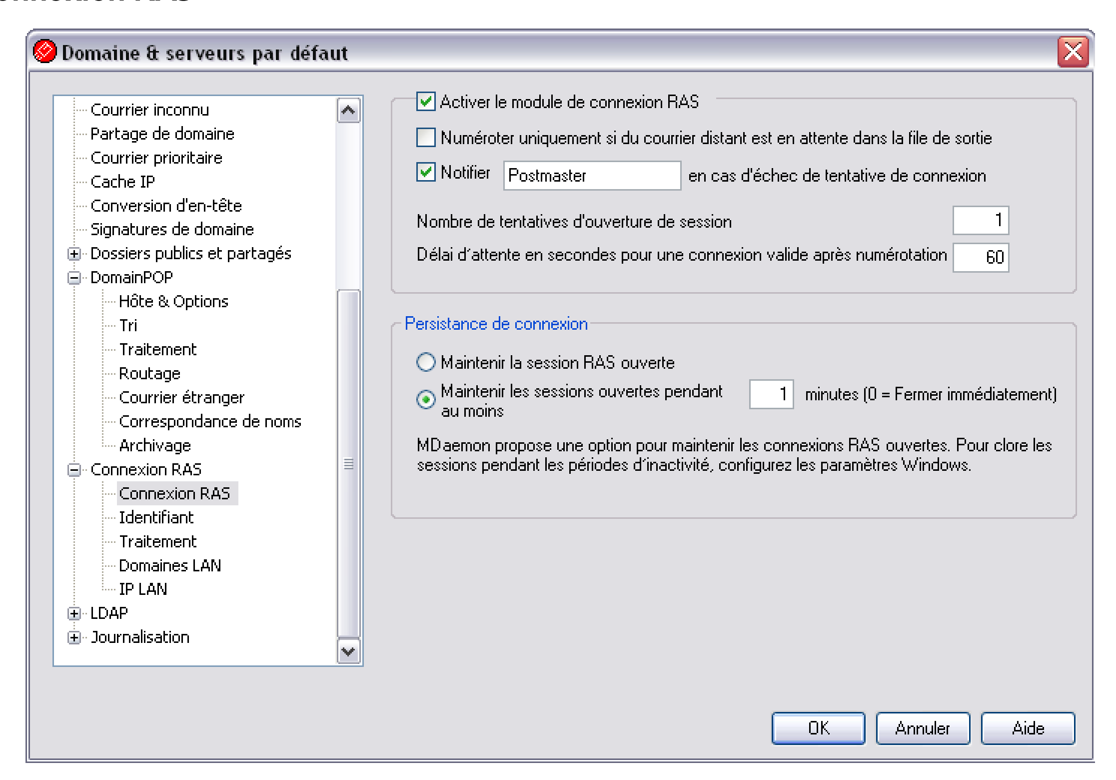
3.1.13 Paramètres de connexion RAS

Pour configurer les paramètres de connexion RAS, cliquez sur "Configuration » Domaine/serveurs par défaut » Connexion RAS". Cette boite de dialogue ne sera disponible que si vous avez installé les services d'Accès distant sur votre système. Ils sont utilisés par MDaemon lorsque vous devez vous connecter à votre FAI pour distribuer le courrier.

Cette section contient 5 onglets :

- Connexion RAS 84
- Identifiant 85
- Traitement 86
- Domaines LAN 87
- IP LAN 88

3.1.13.1 Connexion RAS



Activer le module de connexion RAS
En sélectionnant cette option, MDaemon utilisera les paramètres de cette boîte de dialogue pour établir une connexion avec un serveur distant avant d'envoyer et/ou de recevoir du courrier distant.

Numéroter uniquement si du courrier distant est en attente dans la file de sortie
Lorsque cette option est activée, MDaemon ne se connecte au FAI que si du courrier distant est en attente dans la file distante. Cela peut être utile dans certains cas, mais sachez que si MDaemon ne numérote pas, il ne peut alors pas non plus collecter de courrier (sauf s'il est distribué par le réseau local).

Notifier [adresse] en cas d'échec de tentative de connexion
Lorsque cette option est sélectionnée, MDaemon envoie un message à l'adresse indiquée lorsqu'une connexion échoue pour une raison particulière.

Nombre de tentatives d'ouverture de session
MDaemon tente de se connecter au serveur distant ce nombre de fois avant d'abandonner.

Délai d'attente en secondes pour une connexion valide après numérotation
Cette valeur détermine la durée pendant laquelle MDaemon attend que l'ordinateur distant réponde et établisse la connexion RAS.

Persistance de connexion

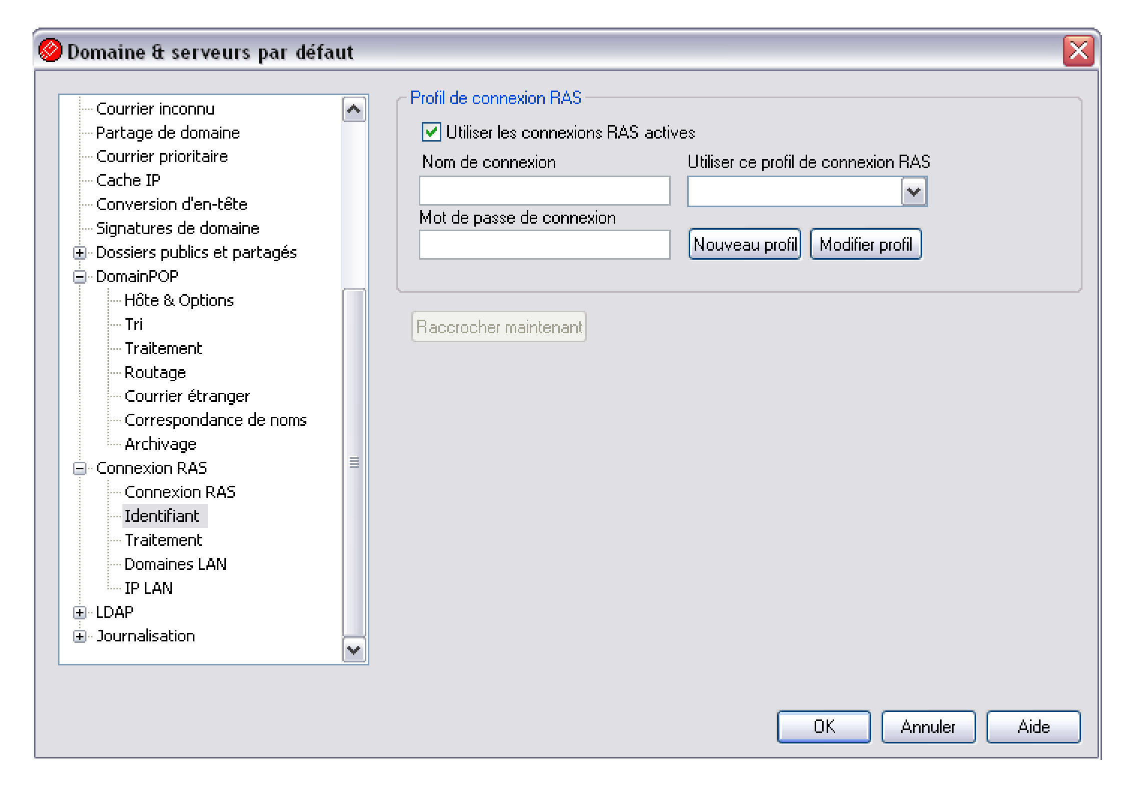
Maintenir la session RAS ouverte
Par défaut, MDaemon ferme immédiatement une connexion créée lorsque toutes les transactions de courrier sont terminées et que la session n'est plus utilisée. En sélectionnant cette option, la connexion reste ouverte même après la fin de toutes les transactions.



MDaemon ne ferme jamais une connexion qu'il n'a pas créée.

Maintenir les sessions ouvertes pendant au moins X minutes
Si vous activez cette option, les sessions RAS créées par MDaemon restent ouvertes pendant, au minimum, le nombre de minutes indiqué, ou jusqu'à ce que toutes les transactions de courrier soient terminées.

3.1.13.2 Identifiant



Profil RAS

Utiliser les connexions RAS actives
Activez cette option si vous voulez que MDaemon puisse utiliser d'autres profils de connexion lorsqu'il détecte qu'une connexion est active. Au moment de se connecter, MDaemon vérifie d'abord s'il peut utiliser une connexion active au lieu

d'en initialiser une nouvelle.

Nom de connexion
La valeur indiquée dans ce champ sera transmise au serveur distant lors de l'authentification.

Mot de passe de connexion
La valeur indiquée dans ce champ sera transmise au serveur distant lors de l'authentification.

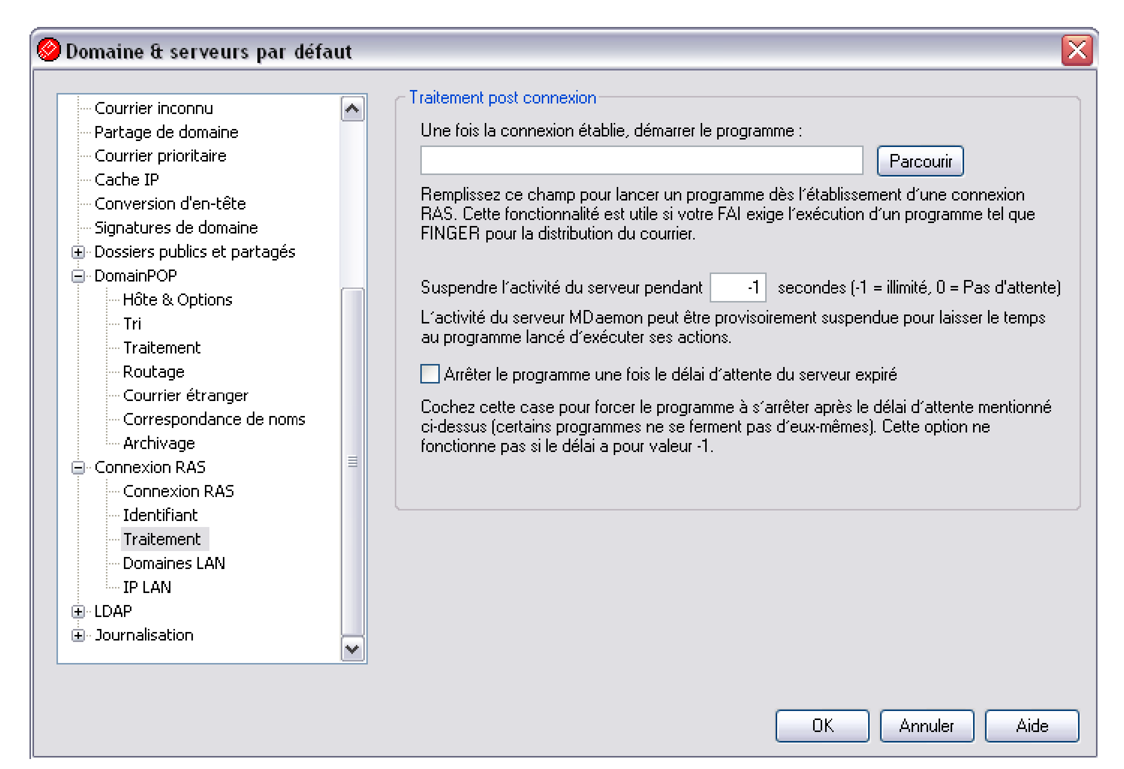
Utiliser ce profil de connexion RAS
Cette liste déroulante permet de sélectionner un profil de session qui a été défini au préalable.

Nouveau profil
Cliquez sur ce bouton pour créer un nouveau profil de connexion.

Modifier profil
Pour modifier un profil, sélectionnez-le et cliquez sur ce bouton.

Raccrocher maintenant
Ce bouton ferme la connexion au FAI. Il n'est disponible que si MDaemon a initié la session RAS.

3.1.13.3 Traitement



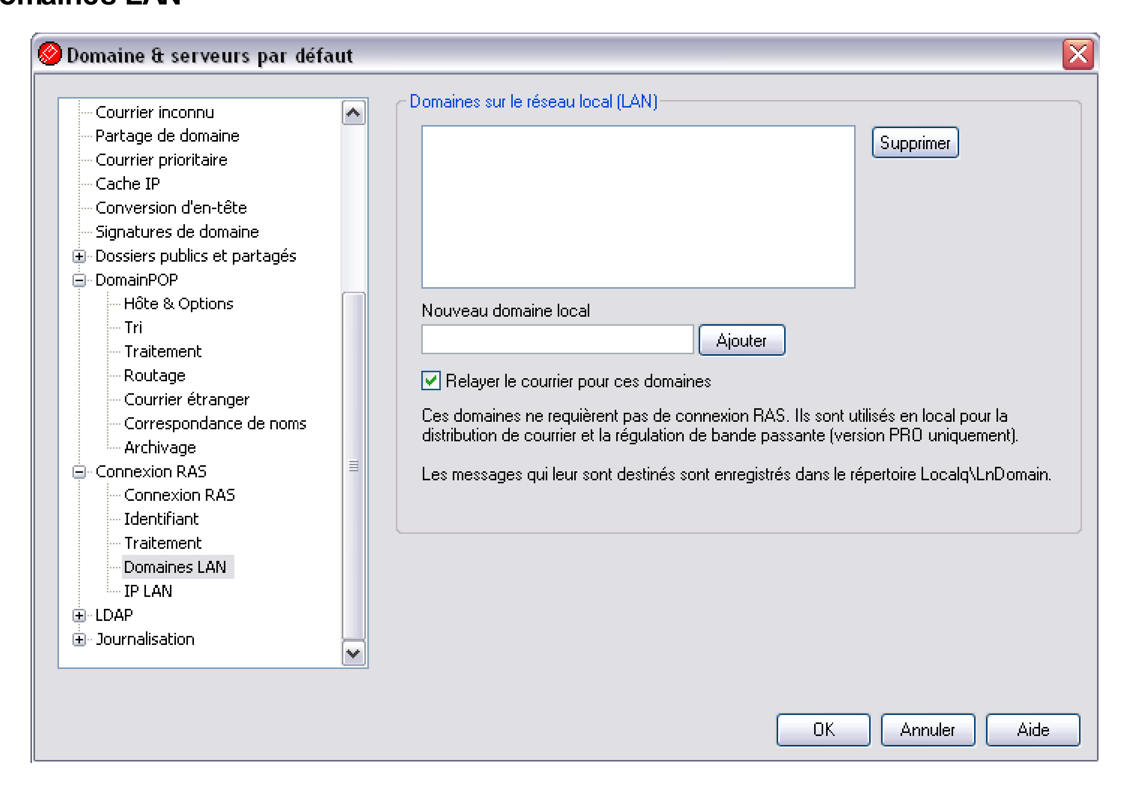
Traitement post connexion

Une fois la connexion établie, démarrer le programme
Si un programme est indiqué dans ce champ, MDaemon l'exécute. Cette fonctionnalité est utile pour les serveurs qui nécessitent Finger ou un autre programme pour retirer le courrier de la boîte aux lettres du FAI.

Suspendre l'activité du serveur pendant X secondes (-1 = illimité, 0=Pas d'attente)
Si l'option ci-dessus contient une entrée valide, le serveur interrompt ses opérations pendant le nombre de minutes indiqué dans ce champ, tout en attendant la fin du processus. En entrant "-1", le serveur attend indéfiniment que le processus se termine.

Arrêter le programme une fois le délai d'attente du serveur expiré
Parfois, le programme que vous avez besoin d'exécuter ne s'arrête pas lorsqu'il a terminé. Certains programmes ne se ferment pas d'eux-mêmes et doivent être forcés à stopper. Si cette option est sélectionnée, MDaemon force le traitement à s'arrêter une fois que le nombre de secondes indiqué dans Suspendre l'activité du serveur pendant secondes est écoulé. Cette option ne fonctionne pas lorsque le serveur est configuré pour attendre indéfiniment la fin du programme.

3.1.13.4 Domaines LAN



Domaines sur le réseau local (LAN)

Les domaines répertoriés dans cette boîte de dialogue sont considérés par MDaemon

comme faisant partie de votre réseau local. Par conséquent, aucune connexion n'est requise pour leur envoyer du courrier.

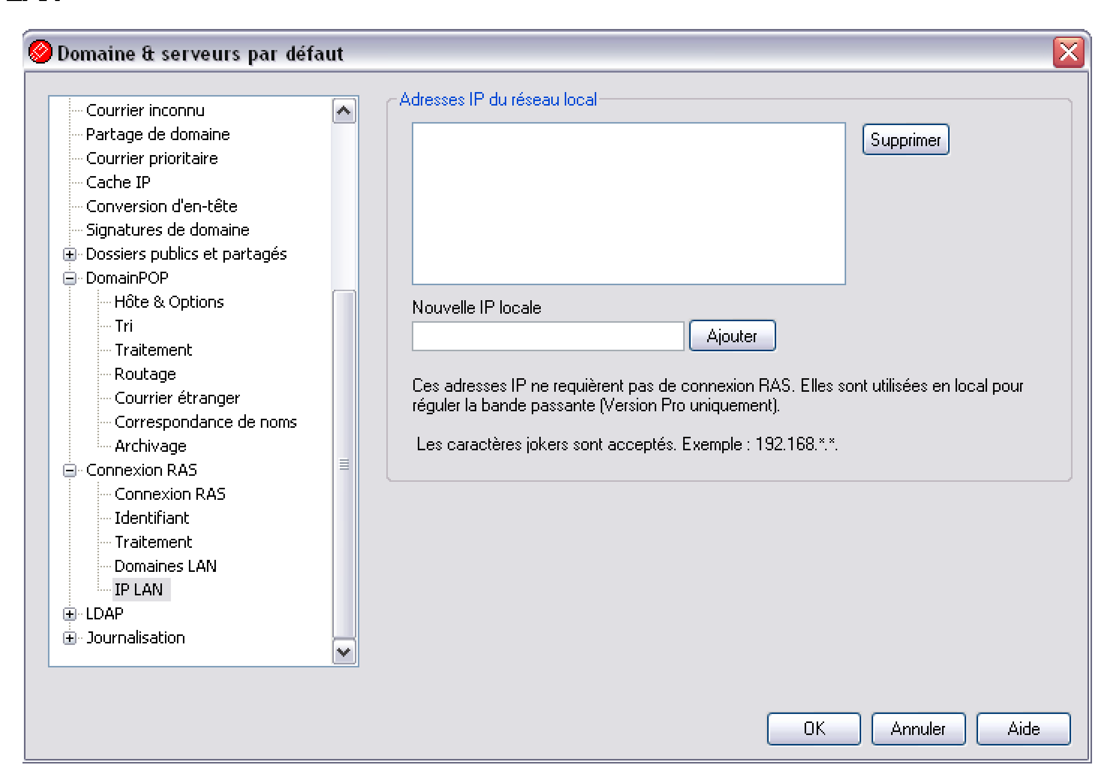
Nouveau domaine local
Entrez un nom de domaine à ajouter à la liste des domaines locaux, puis cliquez sur le bouton Ajouter.

Relayer le courrier pour ces domaines
Si ce paramètre est sélectionné, MDaemon relaie le courrier pour ces domaines. Cela permet de contrôler le trafic à destination et en provenance de ces domaines.

Ajouter
Après avoir rempli les champs ci-dessus, cliquez sur ce bouton pour ajouter une entrée à la liste de vos domaines locaux.

Supprimer
Pour supprimer un domaine de la liste, sélectionnez-le et cliquez sur ce bouton.

3.1.13.5 IP LAN



Adresses IP du réseau local

Tout comme l'onglet Domaines LAN 87, cet onglet sert à répertorier les adresses IP situées sur votre réseau local. Ces IP ne requièrent donc pas de connexion RAS et sont considérées comme locales par le système de régulation de la bande passante. De plus, plusieurs autres restrictions concernant la sécurité et les mesures de

prévention du spam ne sont pas appliquées à ces adresses.

Supprimer
Pour supprimer une adresse IP de la liste, sélectionnez-la et cliquez sur ce bouton.

Nouvelle IP locale
Saisissez une adresse IP à ajouter à la liste des IP locales puis cliquez sur Ajouter. Les caractères jokers tels que 127.0.*.* sont acceptés.

Ajouter
Lorsque vous avez saisi une adresse IP dans le champ ci-dessus, cliquez sur ce bouton pour l'ajouter à la liste.

3.1.14 LDAP/carnet d'adresses

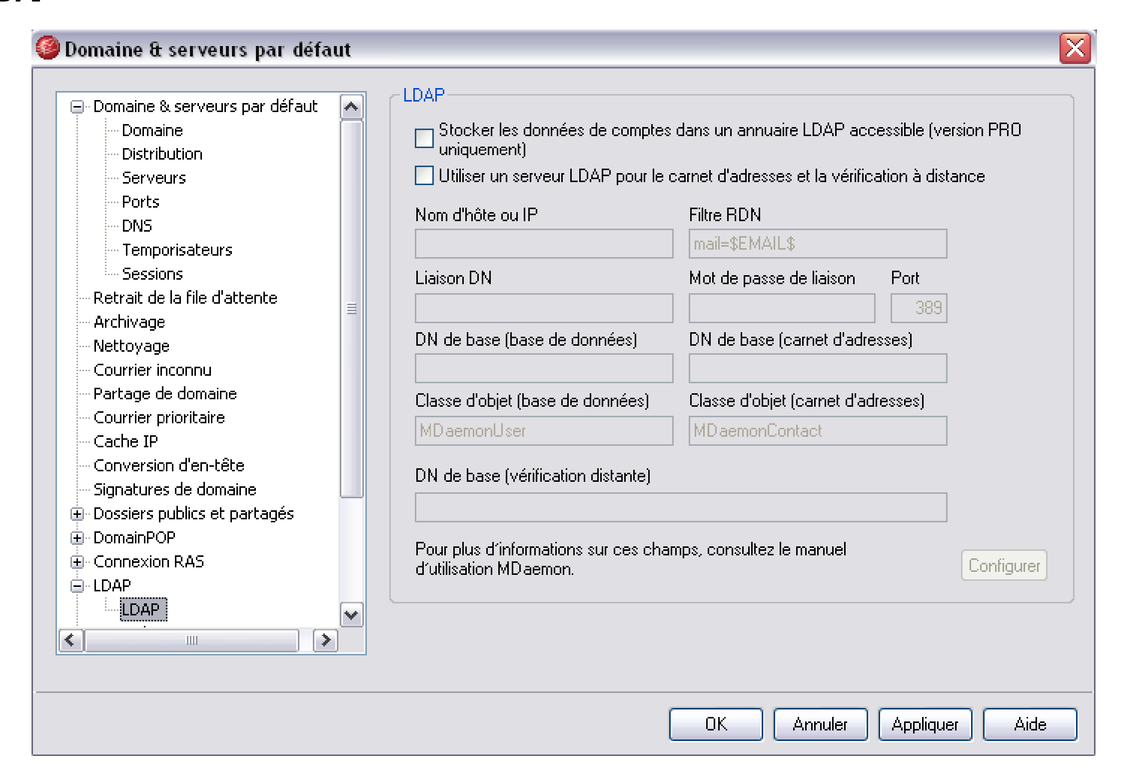
MDaemon supporte le protocole LDAP (Lightweight Directory Access Protocol). Pour accéder aux options LDAP, cliquez sur "Configuration » Domaine/serveurs par défaut » LDAP". MDaemon peut maintenir à jour une base de données LDAP d'utilisateurs, de façon précise et continue, en communiquant avec votre serveur LDAP à chaque fois qu'un compte MDaemon est ajouté ou supprimé. Ainsi, les utilisateurs disposant de clients de messagerie compatibles avec LDAP, peuvent "partager" un carnet d'adresses global. Celui-ci contiendra des entrées pour tous vos utilisateurs MDaemon ainsi que tous les autres contacts que vous y ajouterez.

Vous pouvez également utiliser votre serveur LDAP comme base de données d'utilisateurs MDaemon à la place de son système local USERLIST.DAT ou d'une base de données ODBC. Vous pouvez utiliser cette méthode pour tenir à jour les informations des utilisateurs si vous disposez de plusieurs serveurs MDaemon à des emplacements différents, mais que vous voulez qu'ils partagent une unique base de données utilisateurs. Chaque serveur MDaemon sera configuré pour se connecter au même serveur LDAP afin de partager les informations des utilisateurs au lieu de les stocker localement.

Voir également :

LDAP 90
Base de données des comptes 359

3.1.14.1 LDAP



LDAP

Stocker les données de comptes dans un annuaire LDAP accessible (version PRO uniquement)
Cochez cette case pour que MDaemon utilise votre serveur LDAP comme base de données utilisateurs plutôt qu'une base ODBC ou son système local USERLIST.DAT. Vous pouvez utiliser cette méthode pour tenir à jour vos informations utilisateurs si vous disposez de plusieurs serveurs MDaemon à des emplacements différents, mais que vous voulez qu'ils partagent une unique base de données utilisateurs.

Utiliser un serveur LDAP pour le carnet d'adresses et la vérification à distance
Il est possible que vous utilisiez ODBC ou la méthode par défaut utilisant le système USERLIST.DAT, à la place de la méthode du serveur LDAP pour tenir à jour votre base de données de comptes. Dans ce cas, vous pouvez toujours avoir un serveur LDAP actualisé avec les noms, e-mails et alias de vos utilisateurs, en activant cette option. Ce serveur mis à jour peut ainsi être utilisé comme système de carnet d'adresses global pour les utilisateurs de clients de messagerie compatibles avec les carnets d'adresses LDAP.

Ce système permet de tenir à jour une base de données de vos boîtes aux lettres, alias et listes de diffusion que vos serveurs secondaires peuvent interroger à distance pour vérifier les adresses.

Propriétés du serveur LDAP

Nom d'hôte ou IP
Saisissez ici le nom d'hôte ou l'adresse IP de votre serveur LDAP.

Filtre RDN
Cette option sert à créer le RDN pour l'entrée LDAP de chaque utilisateur. Le RDN (relative distinguished name) est le composant le plus à gauche de chaque DN (distinguished name). Pour toutes les entrées partageant une racine commune, le RDN doit être unique, c'est pourquoi nous vous suggérons d'utiliser l'adresse électronique de chaque utilisateur comme RDN pour éviter tout problème. Si vous utilisez la macro $EMAIL$ comme valeur de l'attribut dans cette commande, (c'est-à-dire mail=$EMAIL$), il sera remplacé par l'adresse électronique de l'utilisateur lorsque son entrée LDAP sera créée. Le DN de l'utilisateur est constitué du RDN et de l'Entrée base DN ci-dessous.

Liaison DN
Saisissez le DN de l'entrée à laquelle vous avez accordé un accès administrateur à votre serveur LDAP, pour que MDaemon puisse ajouter et modifier les entrées de vos utilisateurs MDaemon. Il s'agit du DN utilisé pour l'authentification dans l'opération de liaison.

Mot de passe de liaison
Ce mot de passe sera transmis à votre serveur LDAP avec la valeur Liaison DN pour l'authentification.

Port
Indiquez le port que votre serveur LDAP écoute. MDaemon utilise ce port lorsqu'il envoie des informations de comptes au serveur.

DN de base (base de données)
Saisissez l'entrée base (DN racine) qui sert pour toutes les entrées de vos utilisateurs MDaemon, lorsque vous utilisez le serveur LDAP comme base de données utilisateurs à la place du fichier USERLIST.DAT. L'entrée base DN est associée au RDN (voir Filtres RDN ci-dessus) pour constituer le DN de chaque utilisateur.

DN de base (carnet d'adresses)
Lors de la duplication d'informations de comptes vers un carnet d'adresses de base de données LDAP, saisissez l'entrée base (DN racine) qui sera utilisée pour toutes les entrées de carnets d'adresses de vos utilisateurs MDaemon. L'entrée base DN est associée au RDN (voir Filtres RDN ci-dessus) pour constituer le DN de chaque utilisateur.

Classe d'objet (base de données)
Indiquez la classe objet à laquelle doit appartenir l'entrée de la base de données utilisateurs de chaque titulaire de compte MDaemon. Chaque entrée contiendra l'attribut objectclass= comme valeur.

Classe d'objet (carnet d'adresses)
Indiquez la classe objet à laquelle doit appartenir l'entrée de carnet d'adresses LDAP de chaque utilisateur MDaemon. Chaque entrée contiendra l'attribut objectclass= comme valeur.

DN de base (vérification distante)
Les passerelles de domaine et les serveurs secondaires posent tous les deux le

même problème : habituellement, ils ne proposent aucun moyen de savoir si le destinataire d'un message entrant est valide. Par exemple, si un message destiné à frank@exemple.com arrive sur le serveur secondaire d'exemple.com, il est impossible pour ce serveur de savoir s'il y a effectivement une boîte aux lettres, un alias ou une liste de diffusion pour "frank" sur le domaine exemple.com. Le serveur secondaire est donc obligé d'accepter l'ensemble du courrier. MDaemon dispose d'une méthode qui permet de vérifier les adresses des messages et donc de résoudre ce problème. Il suffit d'indiquer un entrée base DN qui est utilisée pour l'ensemble des boîtes aux lettres, alias et listes de diffusion : toutes ces informations sont ainsi maintenues à jour sur le serveur LDAP. Votre serveur secondaire n'a plus qu'à interroger votre serveur LDAP dès qu'un message entrant est destiné à votre domaine, et à vérifier si l'adresse du destinataire est valable ou pas. Si ce n'est pas le cas, le courrier est rejeté.

Configurer
Cliquez sur ce bouton pour ouvrir le fichier de configuration LDAP.dat dans un éditeur de texte. Il sert à définir les attributs LDAP qui correspondront aux champs des comptes MDaemon.

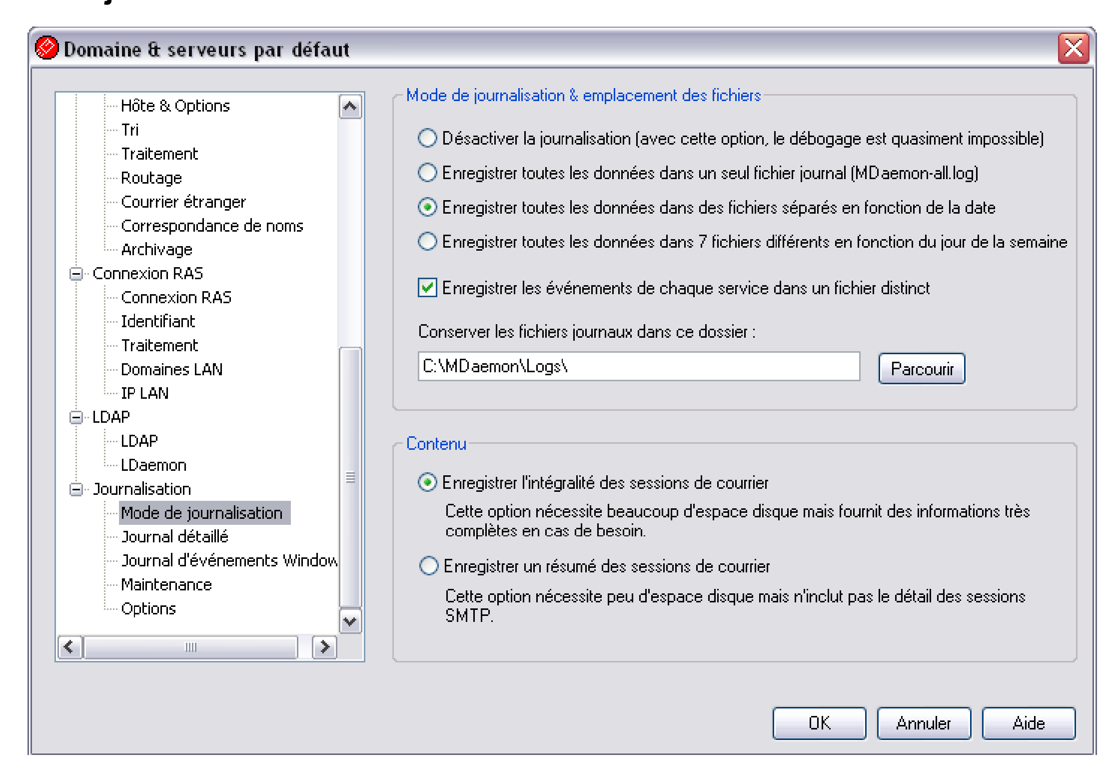
Voir également :

Base de données des comptes 359

3.1.15 Journalisation

Cliquez sur "Configuration » Domaine/serveurs par défaut » Journalisation" pour configurer les paramètres des fichiers journaux. La journalisation est un outil utile qui vous permet de repérer les problèmes et de visualiser l'activité du serveur lorsqu'il n'est pas surveillé.

3.1.15.1 Mode de journalisation

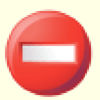




La boîte de dialogue Préférences contient de nombreuses options concernant les données affichées dans les onglets de l'interface principale de MDaemon. Pour en savoir plus, consultez Préférences » GUI 157.

Mode de journalisation & emplacement des fichiers

Désactiver la journalisation
Cette option désactive la journalisation. Les fichiers journaux sont créés mais aucune donnée n'y est enregistrée.



Il est déconseillé d'activer cette option. En effet, sans fichiers journaux il est très difficile, voire impossible de déterminer la cause d'un problème ou d'effectuer un débogage.

Enregistrer toutes les données dans un seul fichier journal (MDaemon-all.log)
Sélectionnez cette option si vous souhaitez que toutes les données soient enregistrées dans un seul fichier appelé `MDaemon-all.log`.

Enregistrer toutes les données dans des fichiers séparés en fonction de la date
Si vous sélectionnez cette option, un fichier journal séparé est créé chaque jour. Le nom de ce fichier correspond à sa date de création.

Enregistrer toutes les données dans 7 fichiers différents en fonction du jour de la semaine
Si vous sélectionnez cette option, un fichier journal séparé est généré pour chaque jour de la semaine. Le nom de ces fichiers correspondra au jour de la semaine où ils ont été crées.

Enregistrer les événements de chaque service dans un fichier distinct
Cochez cette case pour que MDaemon tienne à jour des fichiers journaux séparés pour chaque service. Par exemple, lorsque cette option est activée, MDaemon enregistrera l'activité SMTP dans le fichier MDaemon-SMTP.log, et l'activité IMAP dans le fichier MDaemon-IMAP.log. Vous devez sélectionner cette option lorsque vous exécutez une session de configuration ou Terminal Services de MDaemon afin que les onglets de l'interface affichent les informations enregistrées.

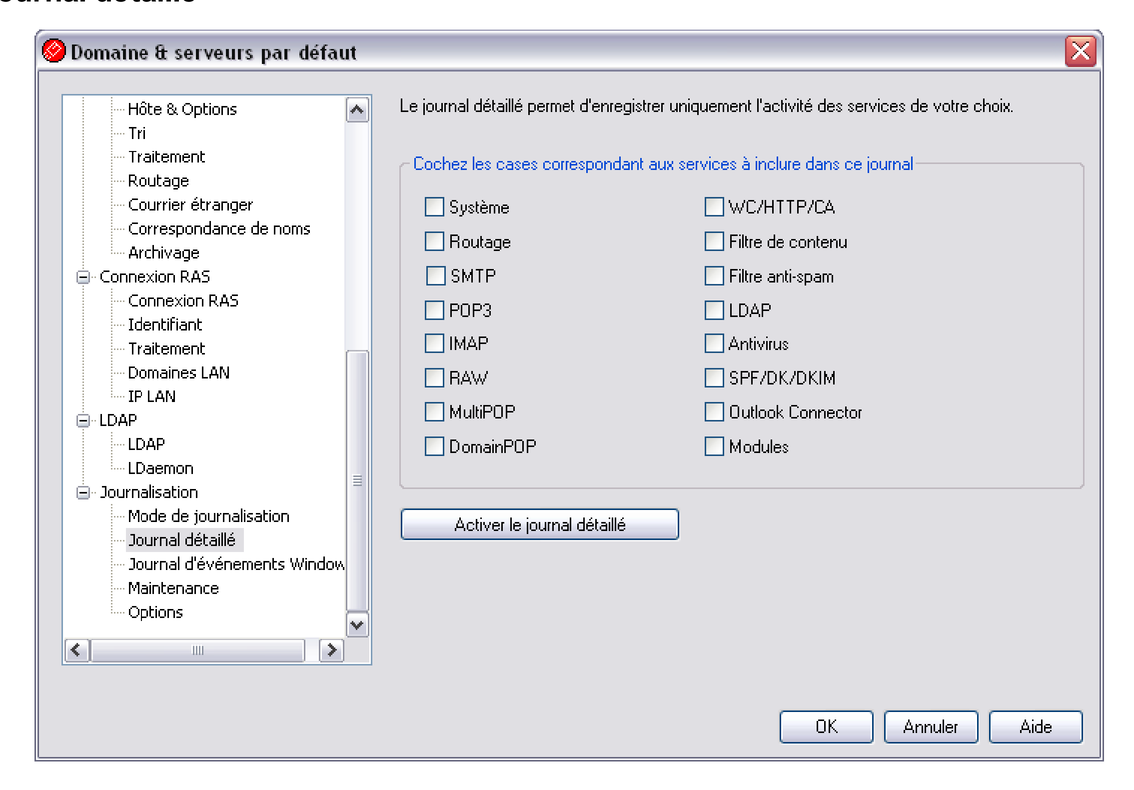
Conserver les fichiers journaux dans ce dossier :
Utilisez cette option si vous souhaitez conserver vos fichiers journaux dans un répertoire spécifique.

Contenu

Enregistrer l'intégralité des sessions de courrier
Un rapport complet de chaque session de courrier est enregistré dans le fichier journal lorsque cette option est activée.

Enregistrer un résumé des sessions de courrier
Avec cette option, un résumé de chaque session de courrier est enregistré dans le fichier journal.

3.1.15.2 Journal détaillé



Journal détaillé

Cochez les cases correspondant aux services à inclure dans ce journal
Le journal détaillé se trouve dans le menu Fenêtres de MDaemon. Il s'affiche dans une nouvelle fenêtre de l'interface principale de MDaemon et inclut les informations contenues dans certains onglets de l'interface principale. Utilisez les options ci-dessous pour déterminer les informations que vous souhaitez inclure :

Système—Activité système de MDaemon : démarrage de services, démarrage/arrêt de serveurs...

Routage—Informations de routage des messages traités par MDaemon (To, From, Message ID, etc.).

SMTP—Détail des sessions SMTP.

POP3—Détail des collectes de courrier à l'aide du protocole POP3.

IMAP—Activité des sessions de courrier IMAP.

RAW—Activité des messages RAW (générés par le système).

MultiPOP—Détail des collectes de courrier MultiPOP.

DomainPOP—Activité DomainPOP de MDaemon.

WorldClient/HTTP/CA—Activité de WorldClient et de la messagerie instantanée ComAgent.

Filtre de contenu—Opérations du Filtre de contenu.

Filtre anti-spam—Activité du filtre anti-spam.

LDAP—Activité LDAP.

Antivirus—Activité de l'antivirus.

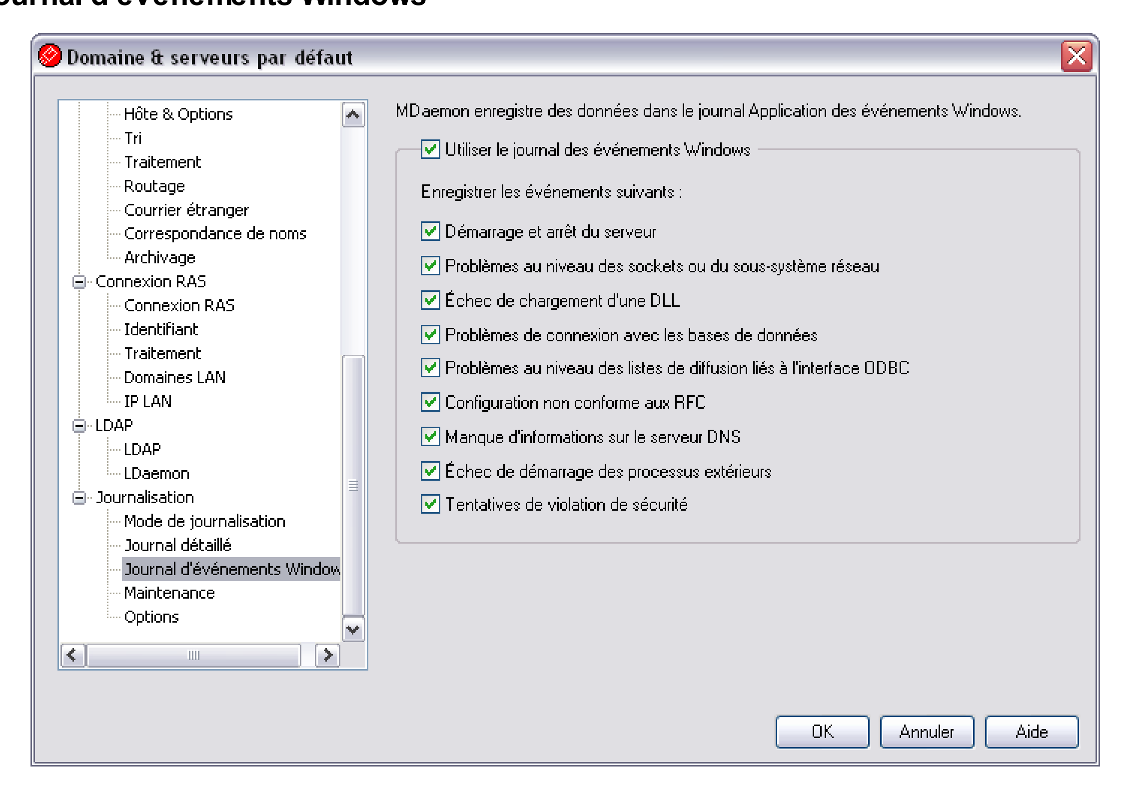
SPF/DK/DKIM—Activité de Sender Policy Framework et DomainKeys.

Outlook Connector—Activité de Outlook Connector.

Modules—Activité des modules personnalisés.

Activer le journal détaillé
Cliquez sur ce bouton pour afficher le journal détaillé dans une nouvelle fenêtre de l'interface de MDaemon.

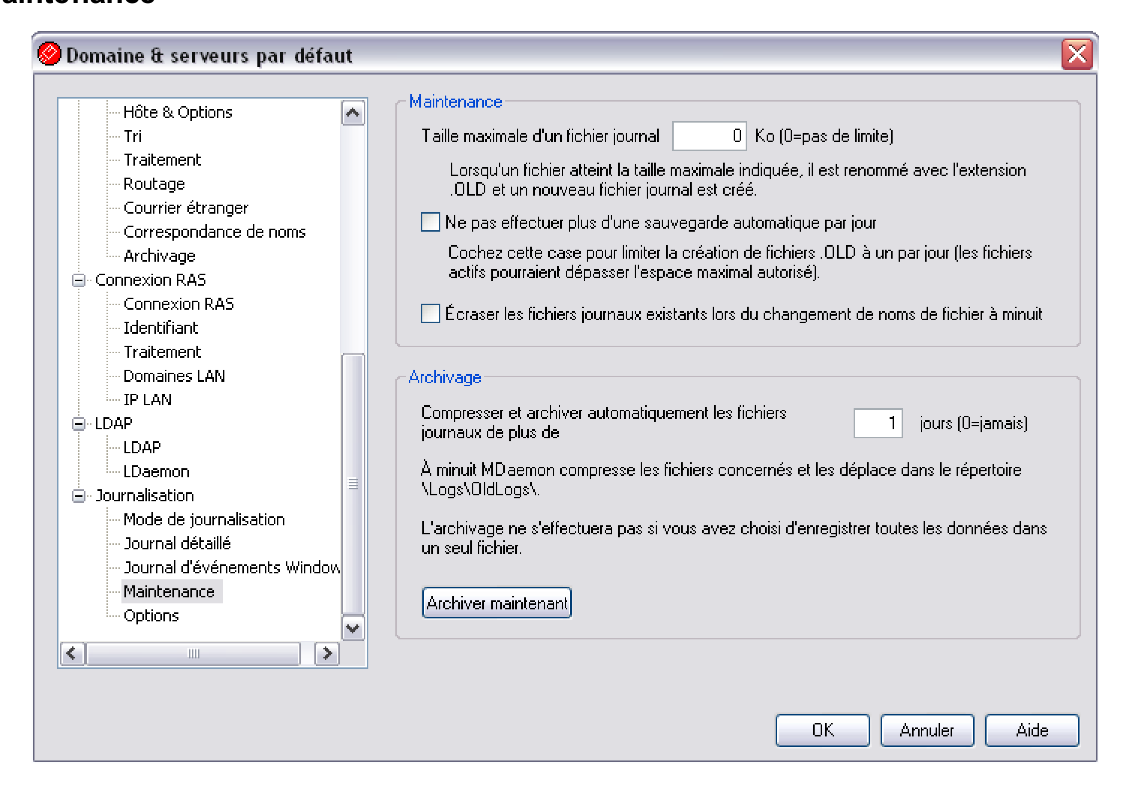
3.1.15.3 Journal d'événements Windows



Utiliser le journal des événements Windows
Activez cette option si vous souhaitez enregistrer les erreurs système critiques, avertissements et autres événements dans la partie Application de l'Observateur d'événements.

Enregistrer les événements suivants :
Si vous enregistrez les événements Windows, utilisez ces différentes options pour spécifier ceux que vous souhaitez enregistrer.

3.1.15.4 Maintenance



Maintenance

Taille maximale d'un fichier journal [xx] Ko
Il s'agit de la taille maximale en Ko d'un fichier journal. Une fois que cette taille est atteinte, le fichier journal est enregistré dans un fichier LOGFILENAME.OLD et un nouveau fichier journal est créé.

Ne pas effectuer plus d'une sauvegarde automatique par jour
Lorsque vous limitez la taille d'un fichier journal, cochez cette case si vous voulez qu'une seule sauvegarde du fichier journal soit effectuée par jour. Chaque jour, lorsque la taille maximale du fichier journal est atteinte pour la première fois, il est renommé "*.OLD" et enregistré normalement. Le fichier journal suivant continuera de croître sans tenir compte de la taille maximale indiquée. Il ne sera pas remplacé avant le jour suivant, même si la taille maximale est dépassée.

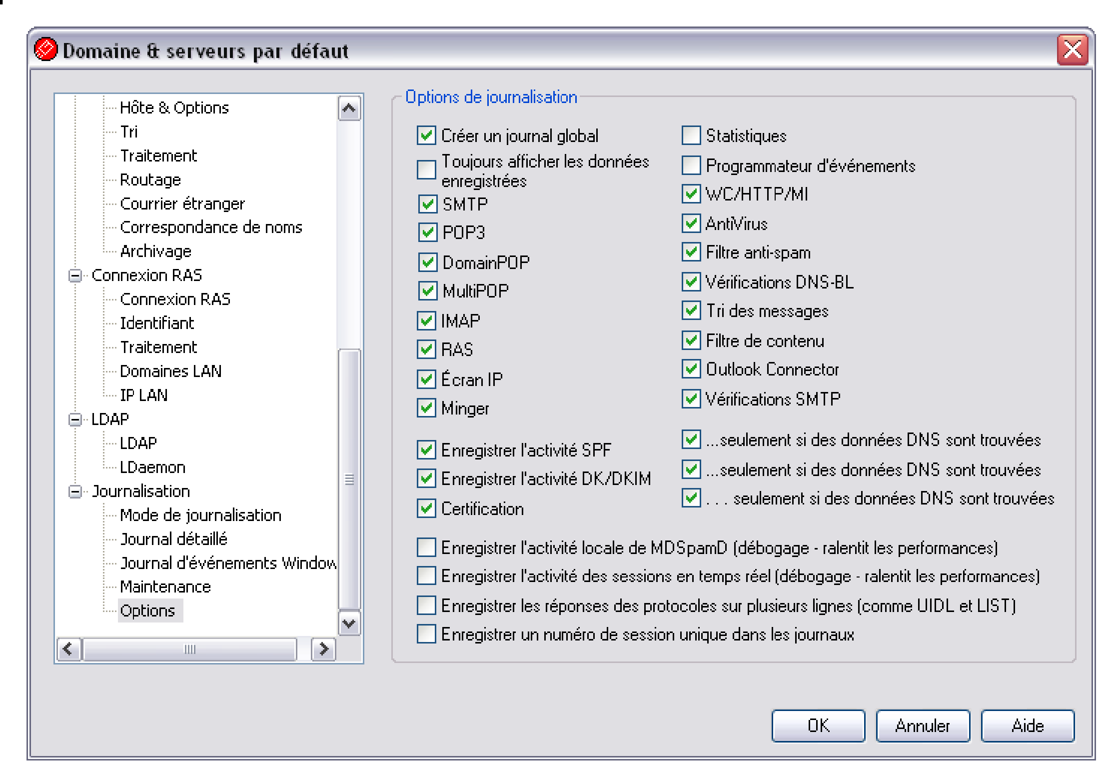
Écraser les fichiers journaux existants lors du changement de noms de fichiers à minuit
Par défaut, lorsque MDaemon modifie le nom d'un fichier journal à minuit et que le nom de remplacement existe déjà, les informations nouvellement enregistrées s'ajoutent au fichier existant. Par exemple, si MDaemon remplace Lundi.log par Mardi.log, et que ce dernier nom de fichier existe déjà, les données enregistrées seront ajoutées à ce fichier existant au lieu de l'écraser ou d'en créer un autre. Par contre, cochez cette case si vous voulez que MDaemon écrase un fichier qui existe, au lieu d'y ajouter les nouvelles données.

Archivage

Compresser et archiver automatiquement les fichiers journaux de plus de XX jours (0 = jamais)
Sélectionnez cette option pour que MDaemon archive les fichiers journaux qui existent depuis plus longtemps que la durée indiquée dans ce champ. Chaque jour, à minuit, MDaemon compresse les fichiers old *.log et *.old, puis les déplace vers le sous-fichier \Logs\OldLogs\ (il supprime les fichiers originaux). Ce processus n'entraîne ni l'archivage, ni la suppression des fichiers qui sont en cours d'utilisation, ni l'archivage des fichiers lorsque l'option Créer un ensemble de fichiers journaux standard est sélectionnée dans l'onglet Mode journal.

Archiver maintenant
Cliquez sur ce bouton pour archiver les anciens fichiers journaux immédiatement, et ne pas attendre que MDaemon les archive automatiquement à minuit.

3.1.15.5 Options



Options de journalisation

Créer un journal global
Crée un fichier appelé "*-all.log" reprenant l'ensemble des activités auditées.

Toujours afficher les données enregistrées
Activez cette option si vous voulez que les données enregistrées soient affichées dans l'interface graphique de MDaemon même lorsqu'elle est réduite ou qu'elle

fonctionne en barre des tâches.

Lorsque cette option est désactivée, les données enregistrées ne sont pas copiées dans les onglets de l'interface principale lorsque MDaemon fonctionne en barre des tâches. Par conséquent, l'activité la plus récente ne sera pas répertoriée dans ces onglets lors de l'ouverture de MDaemon.

SMTP
Activez cette option si vous voulez auditer l'ensemble de l'activité SMTP entrante/sortante de MDaemon.

POP3
Activez cette option pour auditer l'ensemble de l'activité du courrier POP.

DomainPOP
Activité DomainPOP.

MultiPOP
Enregistre l'activité MultiPOP.

IMAP
En activant cette option, toutes les sessions IMAP de vos utilisateurs sont incluses dans les fichiers journaux de MDaemon.

RAS
Enregistre les activités de connexion/déconnexion RAS dans le fichier journal. Ces informations permettent de détecter les problèmes de connexion.

Écran IP
Activité de l'Écran IP.

Minger
Activez cette option si vous voulez que les activités du serveur Minger soient incluses dans le fichier journal de MDaemon.

Statistiques
Cette option est désactivée par défaut car l'enregistrement des statistiques risque d'utiliser beaucoup de ressources et d'espace disque. Activez-la si vous souhaitez tout de même enregistrer les statistiques.

Programmateur d'événements
Enregistre l'activité du Programmateur d'événements 141.

WC/HTTP/IM
Enregistre toute l'activité de WorldClient, HTTP, et de la messagerie instantanée ComAgent. Lorsqu'elle est désactivée, le fichier journal WorldClient et HTTP est créé mais il contient uniquement les heures de démarrage et d'arrêt de WorldClient.

Antivirus
Activité de SecurityPlus for MDaemon.

Filtre anti-spam
Activité du Filtre anti-spam.

Vérifications DNS-BL
Enregistre l'activité des vérifications DNS-BL. En utilisant cette option, vous pouvez visualiser facilement les sites qui ont été inscrits sur liste noire.

Tri des messages
MDaemon analyse périodiquement un grand nombre de messages lorsqu'il doit déterminer les destinataires du courrier. Activez ce paramètre si vous voulez que ces informations soient incluses dans le fichier journal.

Filtre de contenu
Activez cette option si vous voulez inclure l'activité du Filtre de contenu dans le fichier journal.

Outlook Connector
Enregistre l'activité du module Outlook Connector.

Vérifications SMTP
Activez cette option pour enregistrer les sessions SMTP lorsqu'aucun message n'est transmis par le serveur expéditeur (c'est à dire lorsqu'il n'utilise pas la commande DATA).

Enregistrer l'activité SPF
Enregistre l'activité des vérifications SPF.

...seulement si des données DNS sont trouvées
Les vérifications n'ayant pas trouvé de données SPF ne sont pas enregistrées.

Enregistrer l'activité DK/DKIM
Enregistre l'activité DomainKeys/DKIM.

...seulement si des données DNS sont trouvées
Les vérifications n'ayant pas trouvé de données DNS ne sont pas enregistrées.

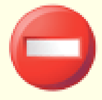
Certification
Enregistre l'activité du système de certification des messages.

…seulement si des données DNS sont trouvées
Activez cette option si vous ne souhaitez enregistrer les données de certification que lorsqu'elles sont présentes dans les DNS.

Enregistrer l'activité locale de MDSpamD (débogage - ralentit les performances)
Enregistre l'activité locale de MDSpamD (voir l'avertissement ci-dessous).

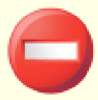
Enregistrer l'activité des sessions en temps réel (débogage - ralentit les performances)
Généralement, les informations des sessions sont enregistrées une fois que la session est terminée afin d'économiser des ressources. Cliquez sur cette option si

vous voulez que les informations des sessions soient auditées en temps réel.



Selon la configuration et l'activité de votre système, les deux options ci-dessus risquent de ralentir ses performances. En règle générale, il est recommandé de ne les utiliser que pour le débogage.

Enregistrer les réponses des protocoles sur plusieurs lignes (comme UIDL et LIST)
Parfois, les réponses à des requêtes de protocole requièrent plus d'une ligne d'informations. Activez cette option si vous voulez enregistrer ces lignes supplémentaires.



En activant cette option, les informations enregistrées augmentent de façon considérable. Dans la mesure où le nombre de lignes dans une réponse peut "remplir" votre fichier journal avec des informations non indispensables (POP TOP, par exemple, qui répertorie le contenu réel du courrier), nous vous conseillons de ne pas utiliser cette option.

Enregistrer un numéro de session unique dans les journaux
Cochez cette option si vous souhaitez intégrer des identifiants uniques [%d:%d] dans les journaux de session.

3.2 Domaines supplémentaires

3.2.1 Héberger plusieurs domaines (MDaemon PRO uniquement)

MDaemon offre une prise en charge complète de plusieurs domaines. En plus des paramètres de configuration du Domaine par défaut32, il inclut l'éditeur de Domaines supplémentaires104 qui sert à désigner autant de domaines supplémentaires que vous voulez prendre en charge, ainsi que l'adresse IP à laquelle chacun d'eux sera associé. MDaemon supporte à la fois les adresses IP dédiées à un seul domaine et celles qui en hébergent plusieurs.

Pour mettre en place le multi-hébergement (plusieurs domaines qui utilisent la même adresse IP), MDaemon détecte automatiquement l'adresse IP qu'une connexion entrante tente d'atteindre et utilise le nom de domaine approprié. Par exemple, supposons que les domaines et les comptes suivants soient configurés :

```
altn.com, IP = 1.1.1.1
utilisateur-1@altn.com, logon = user-1, password = ALTN

arvelh.com - 2.2.2.2
utilisateur-2@arvelh.com, logon = user-2, password = ARVELH
```

Si une tentative de connexion est effectuée vers 1.1.1.1, MDaemon répondra alors en tant que "altn.com". Si une connexion est faite vers 2.2.2.2, alors "arvelh.com" sera

utilisé.

Si utilisateur-1@altn.com se connecte à 1.1.1.1 pour vérifier sa boîte aux lettres, il fournira "utilisateur-1" comme identifiant et "ALTN" comme mot de passe pour se connecter. Toutefois, si utilisateur-2@arvelh.com se connecte à 1.1.1.1 pour vérifier son courrier, il se connecte alors en théorie au mauvais serveur (il devrait se connecter sur 2.2.2.2). Il devra dans ce cas fournir son adresse de messagerie électronique complète dans le champ identifiant pour obtenir l'accès à sa boîte. Bien sûr, s'il s'était connecté sur 2.2.2.2, il aurait seulement eu besoin de fournir son identifiant. Par conséquent, si un compte se connecte à une adresse IP correspondant à son domaine et que cette adresse n'est utilisée par aucun autre domaine, seul l'identifiant doit être indiqué. Sinon, il est nécessaire de préciser une adresse de messagerie complète. Ainsi, il est possible de prendre en charge plusieurs domaines à l'aide d'une seule adresse IP. Lorsque plusieurs domaines partagent la même adresse IP, l'identifiant doit contenir l'adresse de messagerie électronique complète pour que MDaemon puisse déterminer quel utilisateur essaie de se connecter. En cas de doute, entrez l'adresse de messagerie complète pour vous identifier.

Comment sont spécifiés le nom d'identification et le domaine ? Avec l'adresse électronique du compte, la méthode est la suivante : arvel@altn.com. MDaemon acceptera toujours les valeurs du nom d'identification qui contiennent le symbole '@'. Par conséquent, si votre client de messagerie accepte le symbole '@' dans l'identifiant, vous n'aurez pas de problème. Toutefois, de nombreux clients de messagerie sur le marché ne permettent pas l'utilisation du symbole '@' dans le champ d'identification. Pour satisfaire ces clients, MDaemon autorise le remplacement du symbole arobase par le caractère '$'. Autrement dit, vous pouvez utiliser aussi bien arvel$altn.com que arvel@altn.com.

Ce caractère de remplacement est défini dans l'onglet Système 159 de la boîte de dialogue Préférences. La valeur indiquée peut comprendre jusqu'à 10 caractères, ce qui permet de former une chaîne de caractères de délimiteur, au lieu d'utiliser un caractère unique comme '$'. Par exemple, en utilisant '.at.', vous pouvez avoir des valeurs de connexion comme « arvel.at.altn.com ».

Plusieurs fonctionnalités-clés, telles que les Comptes, Listes de diffusion et Paramètres de sécurité sont gérées par domaine. Lorsque vous créez un compte de messagerie, vous devez indiquer le domaine auquel appartient ce nouveau compte. Il en est de même pour les listes de diffusion. Cela signifie que les fonctionnalités telles que l'Écran IP ou le Bouclier IP, sont liées à des domaines de façon individuelle. Toutefois, certaines fonctions comme la Correspondance de noms de DomainPOP, sont liées exclusivement au domaine par défaut.

Afin d'assurer la compatibilité avec les messages système de MDaemon, les alias 347 ci-dessous sont liés par défaut à des boîtes réservées du domaine principal (au lieu d'être liés à chaque domaine secondaire) :

```
MDaemon@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
listserv@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
listserver@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
list-serv@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
```

3.2.2 Domaines supplémentaires

Ajouter un domaine supplémentaire

Pour ajouter un domaine à la liste :

1. Cliquez sur "Configuration » Domaines supplémentaires..."
2. Indiquez le nom du domaine, le nom de domaine complet (FQDN) et son adresse IP.
3. Activez l'option *Lier les sockets d'écoute à cette IP* **uniquement** si vous souhaitez lier le domaine à cette adresse IP.
4. Modifiez les options restantes si nécessaire.
5. Cliquez sur *Ajouter*.

Modifier un domaine supplémentaire

Pour modifier un domaine supplémentaire :

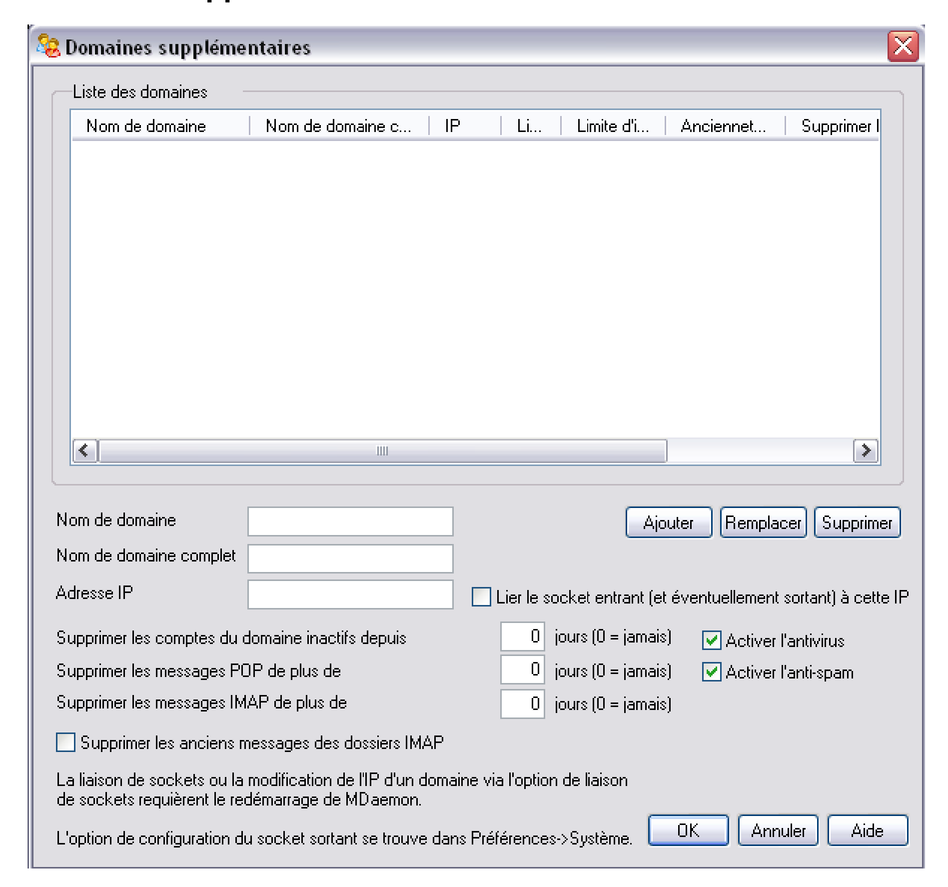
1. Cliquez sur "Configuration » Domaines supplémentaires..."
2. Sélectionnez le domaine à modifier.
3. Effectuez les changements souhaités.
4. Cliquez sur *Remplacer*.

Supprimer un domaine supplémentaire

Pour supprimer un domaine supplémentaire :

1. Cliquez sur "Configuration » Domaines supplémentaires..."
2. Sélectionnez un domaine et cliquez sur le bouton *Supprimer*.

3.2.2.1 Éditeur de domaines supplémentaires



Liste des domaines

Celle-ci peut être triée par ordre croissant ou décroissant dans chaque colonne. Cliquez simplement sur la colonne pour laquelle vous souhaitez que la liste soit triée par ordre croissant. Cliquez à nouveau sur la même colonne pour qu'elle soit triée par ordre décroissant.

Nom de domaine
Saisissez le nom du domaine supplémentaire que vous souhaitez héberger.

Nom de domaine complet
Nom de domaine complet (FQDN) utilisé dans la commande SMTP HELO/EHLO lors de l'envoi de messages pour ce domaine. Pour les connexions entrantes, si l'option *Lier les sockets d'écoute à cette IP* est activée, le domaine est lié à sa propre adresse IP et son nom de domaine complet est utilisé. Il n'est pas nécessaire d'utiliser cette option pour que cela fonctionne. Cependant, si vous possédez plusieurs domaines utilisant la même IP sans liaison ; le nom de domaine complet (FQDN) utilisé sera celui associé au premier domaine par ordre alphabétique.

Dans la plupart des cas, le nom de domaine complet est identique à la valeur *Nom de domaine* ci-dessus ou à un de ses sous-domaines, mais il est également possible d'indiquer une adresse IP sous la forme [1.2.3.4]. Si vous ne remplissez pas ce champ, MDaemon utilise la valeur FQDN du domaine par défaut.

Adresse IP
Entrez l'adresse IP à associer avec le domaine que vous avez ajouté ou modifié.

Lier les sockets d'écoute à cette IP
Cochez cette case si vous souhaitez lier le domaine supplémentaire à son adresse IP. La liaison du socket sortant est contrôlée par une option se trouvant dans Préférences » Système159.

Ajouter
Cliquez sur ce bouton pour ajouter un domaine secondaire avec son adresse IP dans la liste de domaines.

Remplacer
Lorsque vous cliquez sur une entrée de la liste de domaines, ses paramètres s'affichent dans les champs des options correspondantes. Cliquez sur ce bouton après avoir modifié les informations souhaitées afin que les nouveaux paramètres soient pris en compte.

Supprimer
Pour supprimer un domaine de la liste, sélectionnez-le et cliquez sur ce bouton.

Nettoyage de comptes et de messages anciens

Les quatre options ci-dessous se trouvent également dans l'Éditeur de compte317. Les paramètres d'un compte individuel annulent ces paramètres par défaut.

Supprimer les comptes du domaine inactifs depuis X jours (0=jamais)
Indiquez le nombre de jours pendant lequel un compte de ce domaine peut rester inactif avant d'être supprimé. Si vous saisissez la valeur "0" dans le champ de cette option, les comptes ne seront jamais supprimés en raison de leur inactivité.

Supprimer les messages POP de plus de X jours (0=jamais))
Cette valeur correspond au nombre de jours pendant lequel un message peut rester dans la boîte aux lettres d'un utilisateur avant d'être supprimé automatiquement par MDaemon. La valeur "0" signifie que les messages ne seront jamais supprimés en raison de leur ancienneté.

Supprimer les messages IMAP de plus de X jours (0 = jamais)
Utilisez cette option pour indiquer le nombre de jours pendant lequel un message IMAP marqué comme supprimé peut rester dans les dossiers d'un utilisateur de ce domaine. Le courrier ainsi marqué sera supprimé des boîtes aux lettres après le nombre de jours indiqué. La valeur "0" signifie que les messages marqués comme supprimés ne seront jamais supprimés.

Supprimer les anciens messages des dossiers IMAP
Cochez cette case si vous souhaitez que l'option *Supprimer les messages POP...* s'applique également aux dossiers IMAP. Si vous désactivez cette option, les messages contenus dans les dossiers IMAP ne seront pas supprimés, peu importe leur ancienneté.

—

Activer l'antivirus
Si *SecurityPlus for MDaemon* 177 est installé, cochez cette case pour que les paramètres de l'antivirus s'appliquent au domaine sélectionné..

Activer l'anti-spam
Cochez cette case si vous souhaitez que les paramètres actuels du Filtre anti-spam s'appliquent au domaine sélectionné.

Voir également :

Hébergement de plusieurs domaines 101

3.3 Services Web, synchro & MI

3.3.1 WorldClient (web mail)

3.3.1.1 Présentation

WorldClient est inclus dans MDaemon. Il s'agit d'une solution de messagerie Web conçue pour offrir aux utilisateurs un client de messagerie qui utilise leur navigateur Internet favori. Tous leurs dossiers de messagerie sont placés sur le serveur afin que les utilisateurs aient accès à tout ce dont ils ont besoin, comme s'ils étaient au bureau. WorldClient rivalise facilement avec les clients de messagerie traditionnels en offrant en plus aux utilisateurs la possibilité d'accéder à leur courrier électronique en tous lieux et à tous moments.

WorldClient offre de nombreux avantages aux administrateurs de messagerie. Toutes les options se configurent sur le serveur, ce qui évite de devoir configurer chaque client individuellement. Il est également possible d'en personnaliser les images et l'affichage HTML afin d'intégrer votre logo et votre charte graphique. De plus, il est possible d'accorder aux utilisateurs des droits afin de modifier les paramètres de leur compte (les droits accordés sont nombreux et flexibles).

Ce serveur webmail offre également de nombreux avantages : interface disponible presque 30 langues, carnets d'adresses personnels et globaux, dossiers et filtres de courrier, plusieurs "thèmes" pour l'interface, thème pour les périphériques mobiles, calendrier, outils de travail collaboratif, messagerie instantanée, etc.

Système de calendrier et de programmation

MDaemon est pourvu d'un système collaboratif complet. Dans WorldClient, vous créez en toute simplicité des rendez-vous et des carnets d'adresses. Les données des carnets d'adresses, calendriers et tâches sont stockées sous forme de dossiers IMAP dans le dossier racine de chaque utilisateur. Avec WorldClient, chaque utilisateur peut ainsi consulter ses dossiers et accorder des droits d'accès aux autres utilisateurs. Tous les thèmes de WorldClient (en particulier LookOut) affichent les contacts, calendriers, tâches et notes de façon logique et conviviale.

Ce système de calendrier étant intégré dans MDaemon, vous pouvez envoyer par e-mail des notifications de réunions, même si elles ont été planifiées par une tierce

personne. Dès que quelqu'un planifie un rendez-vous pour vous, vous recevez un message qui résume cet événement. Chaque participant concerné reçoit un message précisant la date, l'heure, le lieu, le sujet et la liste des autres participants. En outre, si certains participants possèdent dans leur calendrier des entrées qui coïncident avec le créneau choisi, ils recevront un message leur signalant le conflit entre les différents horaires. La personne qui a programmé la réunion recevra un message récapitulant les renseignements concernant la réunion et les participants conviés ainsi que les éventuels chevauchements.

Le système de calendrier prend également en charge Internet Calendar (iCal) utilisé par Microsoft Outlook et d'autres programmes de messagerie compatibles avec iCalendar. Le système de calendrier peut détecter et traiter des informations iCalendar envoyées à vos utilisateurs, et mettre à jour leurs calendriers en conséquence. Lorsqu'un utilisateur ouvre une pièce jointe iCalendar à partir de WorldClient, les informations qu'elle contient sont dupliquées dans le calendrier WorldClient des utilisateurs. De plus, lorsque des utilisateurs créent des réunions ou des rendez-vous, ils peuvent indiquer une ou plusieurs adresses auxquelles ils souhaitent envoyer un message iCalendar. Cette fonctionnalité peut être configurée par chaque utilisateur dans les options de WorldClient.

ComAgent

ComAgent est un système de messagerie instantanée intégré à MDaemon, fournissant un carnet d'adresses client et une icône dans la barre d'état système qui permet d'accéder rapidement aux fonctionnalités de messagerie de WorldClient. ComAgent peut être téléchargé par chaque utilisateur WorldClient et installé sur son ordinateur local. Il est préconfiguré pour l'utilisateur qui le télécharge, ce qui limite le besoin de le configurer manuellement.

ComAgent s'exécute en arrière-plan et vérifie l'arrivée de nouveaux messages sur votre compte en interrogeant directement WorldClient. Ainsi, il n'est pas nécessaire d'ouvrir un navigateur ou d'en garder un ouvert pour surveiller votre courrier —ComAgent vérifie l'arrivée de nouveaux messages et vous en informe par une alerte sonore ou visuelle. ComAgent affiche également une liste de vos dossiers de messagerie, le nombre et la nature des messages qu'ils contiennent (nouveau, non lu et lu). De plus, vous pouvez l'utiliser pour démarrer votre navigateur et le faire pointer immédiatement vers un dossier de messagerie spécifique, le premier message non lu, la page rédigée ou la page de votre calendrier.

En outre, ComAgent peut effectuer une synchronisation à double sens entre MDaemon et le carnet d'adresses Outlook/Outlook Express, sur l'ordinateur local de chaque utilisateur. Ainsi, si vous utilisez à la fois Outlook ou Outlook Express, et WorldClient à des moments différents, ces carnets d'adresses correspondront dans les deux applications.

Enfin, ComAgent est aussi doté d'un système complet de messagerie instantanée. Vous pouvez visualiser votre liste de contacts ComAgent ainsi que leur statut de connexion (en ligne, absent, déconnecté), démarrer une conversation avec un ou plusieurs utilisateurs, définir votre propre statut de connexion et afficher les anciennes conversations dans un dossier contenant l'historique.

Pour obtenir des informations sur le fonctionnement de ComAgent, consultez son aide en ligne.

Système de messagerie instantanée de ComAgent

ComAgent est doté d'un système de messagerie instantanée (MI) simple mais efficace. Grâce à ce système, vous pouvez communiquer instantanément avec n'importe quel autre compte sur votre serveur MDaemon. Vous pouvez sélectionner une liste de contacts parmi tous les utilisateurs MDaemon, puis voir ceux qui sont en ligne et prêts à recevoir un message instantané. Vous pourrez également démarrer une conversation de groupe réunissant plusieurs personnes à la fois. Toutes les fonctionnalités de la messagerie instantanée sont disponibles dans le menu de raccourcis (clic droit) de ComAgent.

Le système de messagerie instantanée de ComAgent est scriptable. Ainsi, des programmes personnalisés peuvent interfacer avec ce système. En créant des fichiers sémaphore (SEM) dans le répertoire \MDaemon\WorldClient\, une application externe peut envoyer immédiatement des messages instantanés aux utilisateurs de ComAgent. Voici le format du fichier SEM :

`To: frank@example.com`	Adresse e-mail de l'utilisateur de ComAgent.
`From: rip@example.com`	Adresse e-mail de l'expéditeur du message instantané.
`<ligne vide>`	
`Text of instant message.`	Texte du message instantanée.

Le nom du fichier SEM doit commencer par les caractères "IM-" suivis d'une valeur numérique unique. Par exemple, "IM-0001.SEM". Les applications doivent aussi créer un fichier correspondant, nommé "IM-0001.LCK" pour verrouiller le fichier SEM. Une fois que ce fichier SEM est créé, supprimez le fichier LCK et le fichier SEM sera traité. MDaemon utilise cette méthode de cryptage pour vous envoyer des rappels par messagerie instantanée concernant des rendez-vous et des réunions à venir.

Le Filtre de contenu contient une action utilisant cette méthode de cryptage pour envoyer des messages instantanés. De plus, des règles utilisant cette fonction peuvent se servir des macros du Filtre de contenu pour la messagerie instantanée. Par exemple, vous pouvez créer une règle de message instantané qui ressemble à ceci :

```
Vous avez reçu un message de :  $SENDER$.
Subject: $SUBJECT$
```

Cette règle est une méthode efficace pour signaler l'arrivée de nouveaux messages par ComAgent.

De nombreuses entreprises et administrateurs sont réticents à utiliser un système de messagerie instantanée en raison du manque de surveillance centralisée et de l'impossibilité de surveiller le trafic de messagerie instantanée des clients traditionnels connus. Cependant, ce système ne fonctionne pas de poste à poste : les clients individuels de ComAgent ne se connectent pas directement les uns aux autres. Tous les messages instantanés passent par le serveur ; ils sont donc centralisés dans un emplacement accessible à l'administrateur de MDaemon/WorldClient. Il est ainsi possible d'enregistrer toutes les conversations pour la sécurité de votre entreprise et de vos employés ou utilisateurs. L'activité de la messagerie instantanée est enregistrée dans un fichier nommé InstantMessaging.log et situé dans le répertoire MDaemon\LOGS\.

Cette garantie de responsabilité est la raison première pour laquelle MDaemon ne supporte pas les autres clients de messagerie instantanée comme ICQ, AOL et MSN. Enfin, ce système instantanée est entièrement sécurisé : les informations transmis sont cryptées.

La messagerie instantanée se configure par domaine. Les options permettant d'activer la messagerie instantanée et d'indiquer si son trafic doit être enregistré ou non se trouvent dans l'onglet Options de WorldClient ("Configuration » Services Web, Synchro & MI » Options").

Apparences

L'interface de ComAgent est compatible avec les "skins" (apparence) *msstyles* disponibles sur Internet. Plusieurs styles sont inclus par défaut, mais vous pouvez en installer de nouveaux. Pour utiliser le fichier *.msstyles de votre choix, enregistrez-le dans le dossier 'Styles', dans un dossier du même nom. Par exemple, si le nom du fichier est 'Yoda.msstyles', créez un dossier : \Yoda\Yoda.msstyles.

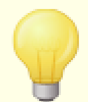
Synchronisation automatique du carnet d'adresses

En utilisant ComAgent avec le système de carnets d'adresses intégré, vous pouvez effectuer une synchronisation à double sens entre MDaemon et un carnet d'adresses Outlook/Outlook Express sur l'ordinateur local de chaque utilisateur. Ainsi, si vous utilisez à la fois Outlook ou Outlook Express, et WorldClient à des moments différents, les carnets d'adresses correspondront dans les deux applications.

MDaemon tient à jour une base de données d'utilisateurs de manière précise et continue : dès qu'un compte MDaemon est ajouté, supprimé ou modifié les informations sont enregistrées. ComAgent consulte MDaemon à intervalles réguliers pour obtenir les informations du contact stockées sur le serveur. Il les publie ensuite dans le carnet d'adresses Windows du poste local ou dans un dossier de contacts. Tous les logiciels locaux qui utilisent ce système de carnet d'adresses sont alors mis à jour instantanément (par exemple, Outlook/Outlook Express).

Tous ceux qui utilisent ComAgent avec des identifiants valides, peuvent également ajouter des contacts publics en utilisant directement le carnet d'adresses Windows ou via Outlook/Outlook Express. Le nouveau contact est alors récupéré par ComAgent et transféré vers le carnet d'adresses de MDaemon. A partir de là, l'ensemble des utilisateurs sur votre réseau ont accès à ce nouveau contact dès que leur système ComAgent consulte MDaemon.

Dans l'onglet *Synchronisation* des propriétés de ComAgent, vous pouvez spécifier les dossiers de votre carnet d'adresses Windows que vous souhaitez synchroniser. Il est possible d'attribuer un dossier spécifique pour les contacts publics et privés.



La synchronisation du carnet d'adresses Windows (WAB) nécessite Internet Explorer 5 ou une version supérieure, avec le support d'identité activé.

Pour plus d'options de carnets d'adresses, voir :

WorldClient (web mail) » ComAgent/MI 119
LDAP 90
Préférences » WAB 366

3.3.1.2 Utilisation de WorldClient

Démarrage de WorldClient

Le serveur WorldClient peut se démarrer/s'arrêter de trois façons différentes :

1. Dans l'onglet Statistiques (à gauche de l'interface principale de MDaemon), effectuez un clic droit sur WorldClient et sélectionnez l'option *Basculer Actif/Inactif.*
2. Cliquez sur le menu "Fichier » Activer le serveur WorldClient".
3. Cliquez sur "Configuration » Services Web, Synchro & MI", et activez l'option *Exécuter WorldClient avec le serveur web intégré.*

Connexion à WorldClient

1. Indiquez dans le navigateur l'URL : `http://example.com:port`. Ce port est indiqué dans l'onglet Serveur Web 111 des paramètres de WorldClient. Si vous configurez WorldClient pour qu'il écoute le port web par défaut (port 80) vous n'avez alors pas besoin d'indiquer le numéro du port dans l'URL de connexion (ex. `www.exemple.com` au lieu de `www.exemple.com:3000`).
2. Entrez votre nom d'utilisateur de compte MDaemon et votre mot de passe.
3. Cliquez sur Connexion.

Modification du numéro de port

1. Cliquez sur "Configuration » Services Web, Synchro & MI".
2. Indiquez le numéro de port souhaité dans le champ *Démarrer WorldClient sur le port TCP.*
3. Cliquez sur OK.

Aide en ligne

WorldClient est doté d'une aide complète pour vos utilisateurs. Consultez cette aide en ligne pour plus d'informations concernant ses fonctionnalités.

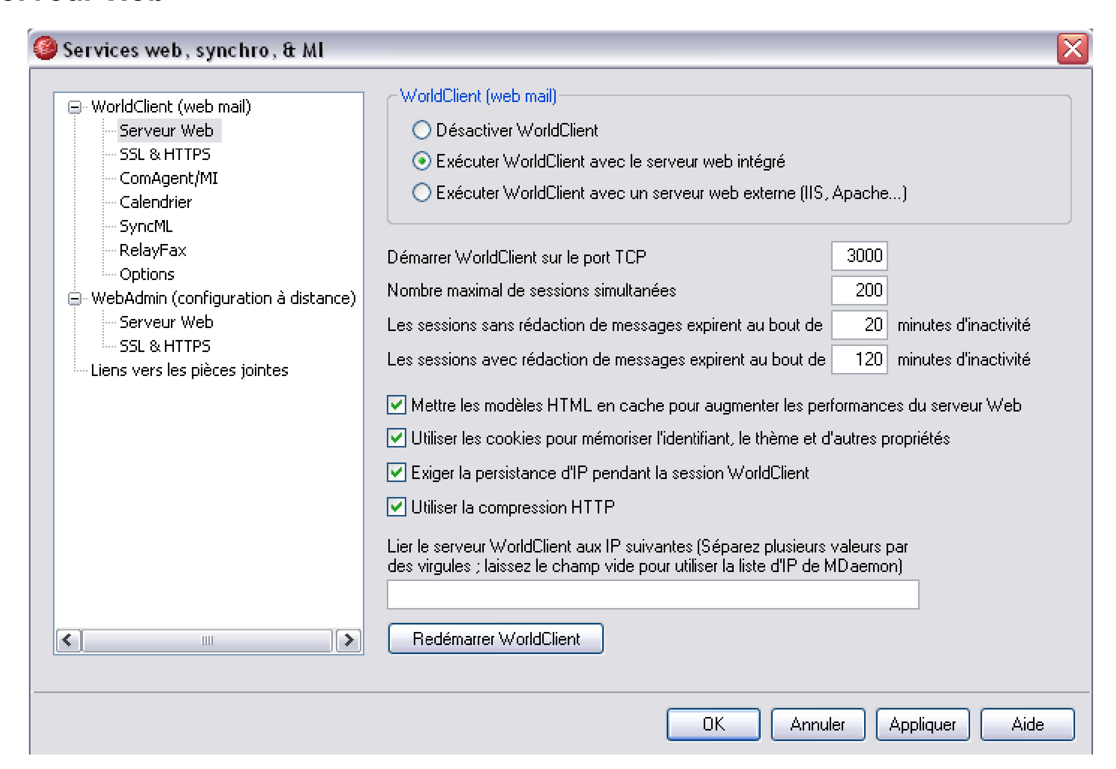
3.3.1.3 WorldClient (webmail)

Pour activer et configurer les paramètres de votre serveur WorldClient, cliquez sur " Configuration » Services Web, Synchro & MI » WorldClient (web mail). Vous pouvez indiquer le port sur lequel il fonctionne, ainsi que le laps de temps pendant lequel les sessions WorldClient peuvent rester inactives avant d'expirer. Vous pouvez également contrôler de nombreux paramètres généraux ou spécifiques à un domaine : la langue et le thème à utiliser par défaut, la pagination par défaut de la liste de messages, de nombreuses fonctionnalités de Calendrier et de Programmation, des paramètres de carnets d'adresses publics et privés, l'intégration de RelayFax etc. Vous pouvez définir si les utilisateurs peuvent ou non créer des comptes, si la prise en charge de ComAgent est activée ou non, si l'envoi de messages instantanés est autorisé et si ceux-ci sont enregistrés, et bien d'autres options encore.

Cliquez sur l'un des liens ci-dessous pour en savoir sur les différentes options de WorldClient :

Serveur web 111
SSL / HTTPS 116
Calendrier 120
SyncML 122
RelayFax 124
Options 126

3.3.1.3.1 Serveur Web



Cet onglet contient plusieurs paramètres généraux du serveur qui régissent la configuration et le comportement de WorldClient sans tenir compte des utilisateurs ou des domaines auxquels ils appartiennent.

Propriétés de WorldClient

Désactiver WorldClient
Vous pouvez également activer/désactiver WorldClient dans le menu Fichier ou bien dans l'onglet Statistiques de l'interface principale.

Exécuter WorldClient avec le serveur web intégré
Cochez cette option pour exécuter WorldClient avec le serveur web intégré de MDaemon.

Exécuter WorldClient avec un serveur web externe (IIS, Apache, etc)
Cochez cette option si vous souhaitez exécuter WorldClient sous IIS ou tout autre serveur web. Cela bloque l'accès à certaines options qui pourraient entraîner un conflit avec votre serveur.

Pour plus d'informations, voir Exécuter WorldClient sous IIS 113

Démarrer WorldClient sur le port TCP
Il s'agit du port sur lequel WorldClient écoute les connexions depuis les navigateurs Web de vos utilisateurs.

Nombre maximal de sessions simultanées
Il s'agit du nombre maximum de sessions pouvant être connectées à WorldClient en même temps.

Les sessions sans rédaction de message expirent au bout de X minutes d'inactivité
Lorsqu'un utilisateur est connecté à WorldClient mais ne rédige pas de message, la valeur saisie ici correspond au temps d'inactivité autorisé avant que WorldClient ne ferme cette session.

Les sessions avec rédaction de message expirent au bout de X minutes d'inactivité
Ce temporisateur contrôle la durée pendant laquelle la session d'un utilisateur est maintenue ouverte pendant qu'il rédige un message et que la session reste inactive. De préférence, fixez une durée supérieure à celle du temporisateur *Les sessions sans rédaction de message…*, puisque le temps d'inactivité est plus important lorsqu'un utilisateur rédige un message. En effet, la rédaction d'un message ne nécessite aucune communication avec le serveur jusqu'à ce que le courrier soit envoyé.

Mettre les modèles HTML en cache pour augmenter les performances du serveur Web
Activez cette option pour que WorldClient mette en cache les modèles et éviter de les recharger à chaque fois que l'on doit y accéder. Cela peut augmenter considérablement les performances du serveur mais il est nécessaire de redémarrer WorldClient si vous procédez à des modifications dans l'un des fichiers de modèles.

Utiliser les cookies pour mémoriser l'identifiant, le thème et d'autres propriétés
Sélectionnez cette option pour que WorldClient stocke l'identifiant, le thème et d'autres propriétés de l'utilisateur dans un cookie sur son ordinateur local. Ainsi, les

utilisateurs disposent d'un profil de connexion personnalisé. Cela nécessite toutefois que les cookies soit acceptés par le navigateur.

Exiger la persistance d'IP pendant la session WorldClient
Pour plus de sécurité, vous pouvez activer cette option afin que WorldClient restreigne chaque session utilisateur à l'adresse IP à partir de laquelle l'utilisateur se connecte au début de la session. Ainsi, personne ne peut "voler" la session de l'utilisateur puisque la persistance d'IP est requise. Cette configuration est sécurisée mais elle peut poser des problèmes aux utilisateurs qui utilisent un serveur proxy ou un compte d'accès par ligne commutée qui attribue et modifie de façon dynamique les adresses IP.

Utiliser la compression HTTP
Cochez cette case si vous souhaitez utiliser la compression HTTP lors de vos sessions WorldClient.

Lier le serveur web WorldClient aux IP suivantes
Si vous voulez limiter l'accès au serveur WorldClient à certaines adresses IP seulement, indiquez-les ici en les séparant par des virgules. Si ce champ est vide, WorldClient surveille toutes les adresses IP que vous avez indiquées pour le domaine principal et les domaines supplémentaires.

Redémarrer WorldClient (obligatoire si modification de port ou de valeur ISS)
Cliquez sur ce bouton si vous souhaitez redémarrer WorldClient. Remarque : lorsque vous modifiez le numéro de port de WorldClient, vous devez redémarrer WorldClient afin que la nouvelle configuration soit prise en compte.

3.3.1.3.1.1 Exécuter WorldClient sous IIS 6

WorldClient est doté d'un serveur Web intégré et, par conséquent, il ne nécessite pas IIS (Internet Information Server). Toutefois, WorldClient supporte IIS et peut donc fonctionner comme une DLL ISAPI. Pour configurer WorldClient afin qu'il fonctionne sous IIS (extrait de l'article #01465 de la base de connaissances MDaemon d'Alt-N) :

1. Ouvrez le gestionnaire des services Internet.
2. Effectuez un clic droit sur **Pools d'application**.
3. Sélectionnez **Nouveau/ Pool d'application**.
4. Appelez-le **Alt-N** et cliquez sur **OK**.
5. Effectuez un clic droit sur **Alt-N** et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Performances.**
7. Décochez les options **Arrêter les processus de travail après une inactivité de** et **Limiter la file d'attente de demandes du noyau**.
8. Cliquez sur l'onglet **Identité.**
9. Dans le menu déroulant **Prédéfini**, sélectionnez **Service local**.
10. Cliquez sur **OK.**

11. Effectuez un clic droit sur **Sites Web**.
12. Sélectionnez **Nouveau/Site Web** (cela ouvre un assistant).
13. Cliquez sur **Suivant**.
14. Choisissez un nom pour le site, par exemple **WorldClient.**
15. Cliquez sur **Suivant**.
16. Ne modifiez pas la fenêtre qui suit et cliquez directement sur **Suivant**.
17. Indiquez le chemin d'accès au répertoire de base. Par défaut : **C:\MDaemon\WorldClient\HTML**.
18. Cliquez sur **Suivant**.
19. Assurez-vous que les options **Lecture**, **Exécuter** et **Exécuter les scripts** soient cochées.
20. Cliquez sur **Suivant** puis sur **Terminer**.
21. Effectuez un clic droit sur le site que vous venez de créer **(WorldClient).**
22. Cliquez sur **Propriétés.**
23. Cliquez sur l'onglet **Documents.**
24. Supprimez tous les documents figurant dans la liste.
25. Ajoutez **WorldClient.dll.**
26. Cliquez sur l'onglet **Répertoire de base**.
27. Dans le menu déroulant Pool d'applications, sélectionnez **Alt-N**.
28. Cliquez sur **OK**.
29. Cliquez sur **Extensions du service Web**.
30. Autorisez **Toutes les extensions ISAPI inconnues** ou bien ajoutez une nouvelle extension pour **WorldClient.DLL.**

Le compte invité Internet (IUSER_<NOMDUSERVEUR>) doit posséder toutes les permissions NTFS pour le répertoire MDaemon et tous ses sous-répertoires.Pour cela :

1. Effectuez un clic droit sur le répertoire MDaemon (par défaut : C:\MDaemon)
2. Sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Sécurité**.
4. Cliquez sur le bouton **Ajouter.**
5. Cliquez sur le bouton **Avancé**.
6. Cliquez sur **Rechercher**.
7. Sélectionnez **IUSER_<NOMDUSERVEUR>** (en remplaçant <NOMDUSERVEUR> par le nom de l'ordinateur).
8. Cliquez sur **OK** dans les fenêtres ouvertes.
9. Cochez la case **Contrôle total**.
10. Cliquez sur **OK.**



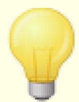
Ces étapes doivent être appliquées à tous les répertoires utilisés par MDaemon.

Pour effectuer les mises à jour de MDaemon :

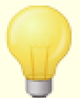
1. Ouvrez le gestionnaire des services Internet.
2. Cliquez sur **Pool d'applications**.
3. Effectuez un clic droit sur **Alt-N**.
4. Sélectionnez **Arrêter**.
5. Arrêtez MDaemon.
6. Installez la nouvelle version.
7. Une fois l'installation terminée, démarrez MDaemon.
8. Effectuez à nouveau un clic droit sur **Alt-N** dans le gestionnaire de services Internet.
9. Sélectionnez **Démarrer**.

Une fois cette opération terminée :

1. Après avoir fermé la console **Pool d'applications** un message "Service indisponible" s'affiche pour les utilisateurs.
2. Cette procédure évite de devoir redémarrer l'ordinateur après avoir effectué la mise à jour.

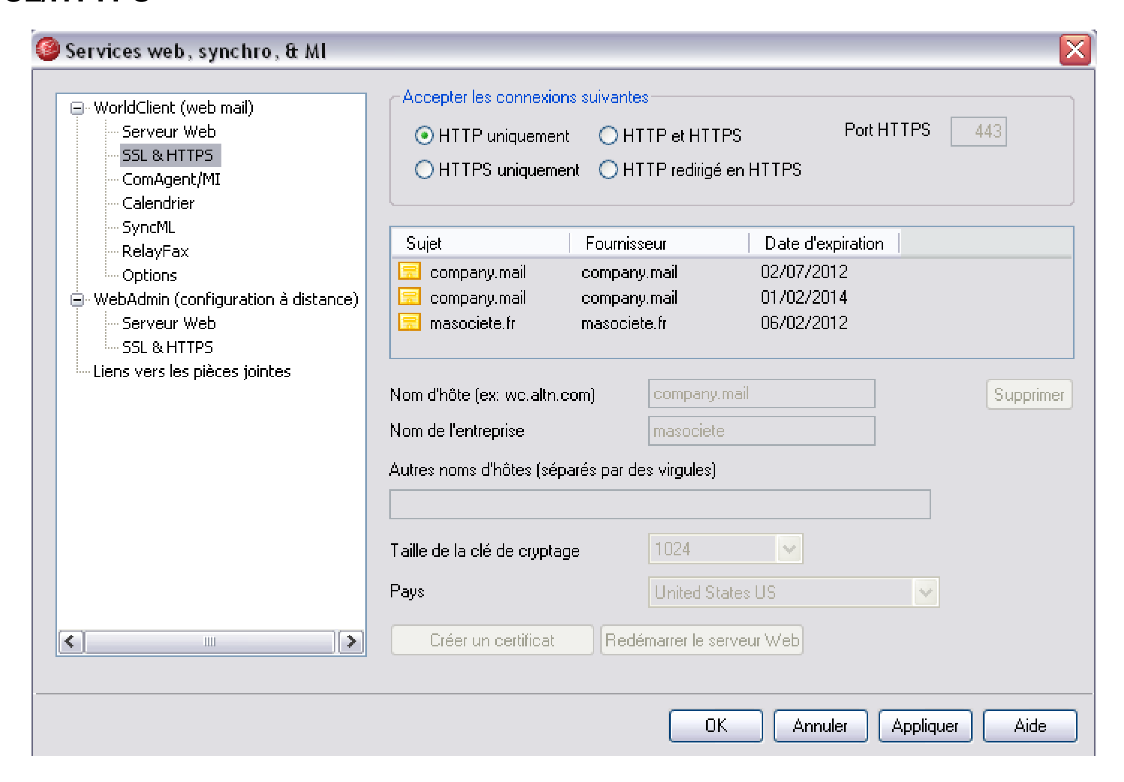


La configuration de ce programme sous IIS N'EST PAS prise en charge par le support technique. Les utilisateurs souhaitant exécuter WorldClient sous IIS doivent s'informer des implications et problèmes de sécurité liés à IIS. Il est recommandé d'installer tous les patches et mises à jour de IIS avant d'installer WorldClient en tant qu'extension ISAPI.



Lorsque vous exécutez WorldClient sous IIS, vous ne pourrez plus le démarrer ni l'arrêter à partir de l'interface de MDaemon. Pour cela, vous devrez utiliser les outils fournis avec IIS.

3.3.1.3.2 SSL/HTTPS



Le serveur Web de MDaemon supporte le protocole SSL (Secure Sockets Layer). Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il fournit l'authentification du serveur, le cryptage de données, et l'authentification facultative du client pour la connexion TCP/IP. De plus, dans la mesure où SSL est intégré aux principaux navigateurs actuels, en installant simplement un certificat numérique valide sur votre serveur, les fonctions SSL du client qui se connecte sont activées.

Les options relatives à l'activation et à la configuration de WorldClient pour qu'il utilise le protocole SSL/HTTPS, se trouvent dans la boîte de dialogue SSL & HTTPS (Configuration » Services web, synchro & MI » WorldClient (webmail)". Pour plus de commodité, ces options sont également accessibles dans la boîte de dialogue "Sécurité » Paramètres de sécurité » SSL & TLS » WorldClient".

Pour en savoir plus sur ce protocole, voir : **SSL & certificats** 271



Les éléments de cette boîte de dialogue s'appliquent uniquement lorsque WorldClient utilise le serveur web intégré de MDaemon. Si vous avez configuré WorldClient pour fonctionner sur un autre serveur, ces options ne seront alors pas utilisées—le support SSL/HTTPS doit être configuré dans le serveur choisi.

Accepter les connexions suivantes

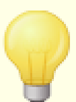
HTTP uniquement
Sélectionnez cette option si vous ne souhaitez pas autoriser les connexions HTTPS à WorldClient. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS
Cette option accepte le support SSL pour WorldClient, mais les utilisateurs ne sont pas obligés d'employer des connexions HTTPS. Dans ce cas WorldClient écoute les connexions HTTPS sur le port indiqué ci-dessous, mais il répond également aux connexions HTTP normales.

HTTPS uniquement
Avec cette option, il est obligatoire d'utiliser une connexion HTTPS pour se connecter à WorldClient. Les requêtes HTTP ne sont pas acceptées.

HTTP redirigé en HTTPS
Sélectionnez cette option pour rediriger toutes les connexions HTTP sur le port HTTPS.

Port HTTPS
Il s'agit du port TCP que WorldClient écoutera pour les connexions SSL. Le port SSL par défaut est le port 443. Si le port SSL par défaut est utilisé, vous n'aurez pas à inclure le numéro du port dans l'URL de WorldClient lors de la connexion par HTTPS (https://exemple.com est équivalent à https://exemple.com:443).



Le port HTTPS n'est pas le même que celui indiqué dans l'onglet Serveur Web111 des propriétés de WorldClient. Si vous autorisez toujours les connexions HTTP vers WorldClient, ces connexions devront alors utiliser cet autre port pour pouvoir être effectuées correctement. Les connexions HTTPS doivent utiliser le port HTTPS.

Certificats

Cette boîte présente vos certificats SSL. Cliquez une fois sur un certificat pour le sélectionner et l'utiliser. Double-cliquez sur un certificat pour visualiser les détails le concernant dans la boîte de dialogue Certificat.



MDaemon ne permet pas à WorldClient d'utiliser plusieurs certificats. Tous les domaines de WorldClient doivent donc partager un même certificat. Si vous avez plusieurs domaines WorldClient, entrez leur nom (et celui des autres domaines auxquels vous souhaitez autoriser l'accès à WorldClient) dans le champ *Autres noms d'hôtes*, situé en dessous.

Supprimer
Sélectionnez un certificat dans la liste puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous voulez vraiment

supprimer ce certificat.

Nom d'hôte
Saisissez le nom de l'hôte auquel vos utilisateurs se connecteront (par exemple, « courrier.exemple.com »).

Nom de l'entreprise
Saisissez le nom de l'organisme ou de la société "propriétaire" du certificat.

Autres noms d'hôtes (séparés par des virgules)
Actuellement, MDaemon ne permet pas à chaque domaine WorldClient de posséder son propre certificat : ils doivent donc tous partager le même. Saisissez dans ce champ, en les séparant par des virgules, les noms des autres domaines auxquels les utilisateurs se connecteront et auxquels le certificat s'appliquera. Les caractères jokers sont acceptés. Ainsi, "`*.exemple.com`" s'appliquera à tous les sous-domaines d'`exemple.com` (par exemple, "`wc.exemple.com`", "`mail.exemple.com`", etc).

Taille de la clé de cryptage
Choisissez la longueur, en bits, de la clé de cryptage pour ce certificat. Plus la clé de cryptage est longue, plus le transfert des données est sécurisé. Veuillez noter que toutes les applications ne supportent pas toutes des clés de plus de 512 bits.

Pays
Indiquez dans quel pays se trouve votre serveur.

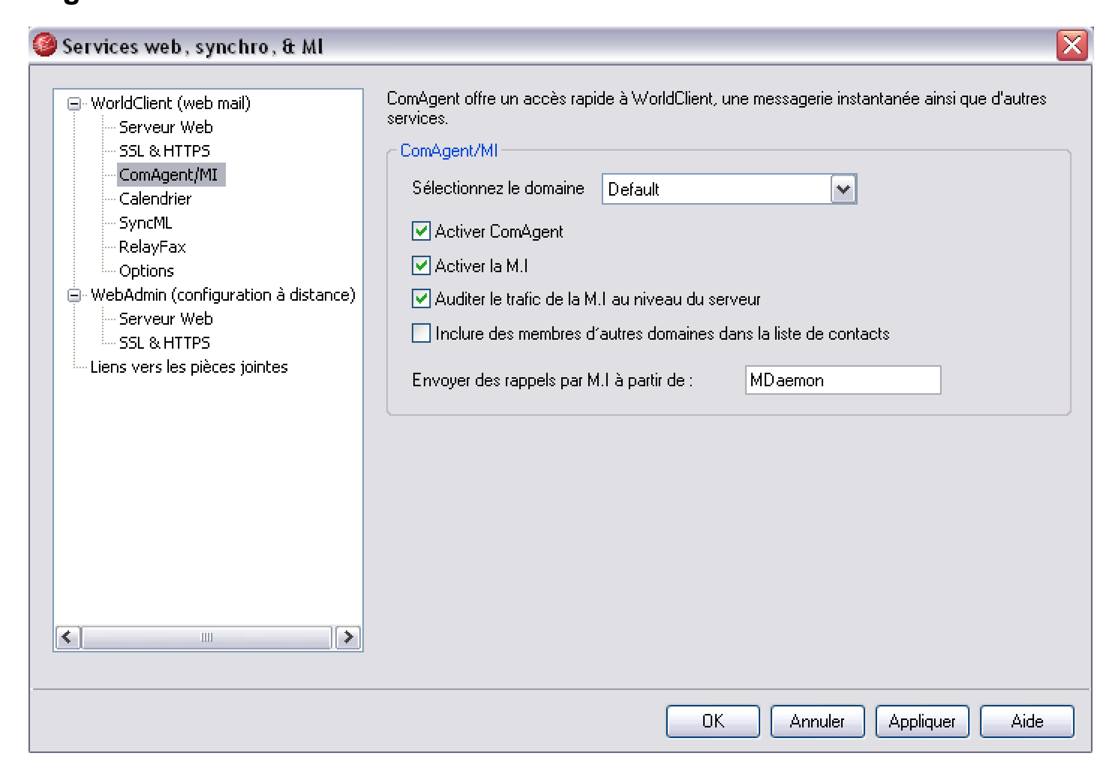
Créer un certificat
Lorsque vous avez saisi toutes les informations requises dans les champs précédents, cliquez sur ce bouton pour créer votre certificat.

Redémarrer le serveur Web
Cliquez sur ce bouton pour redémarrer WorldClient. Il doit être relancé avant l'utilisation des nouveaux certificats.

Voir également :

SSL & Certificats 27
Création et utilisation de certificats SSL 28

3.3.1.3.3 ComAgent/MI



Configurez ici les options de l'utilitaire ComAgent. Ces options peuvent être différentes pour chaque domaine.

ComAgent/MI

Sélectionnez le domaine
Utilisez cette liste déroulante pour choisir le domaine dont vous souhaitez modifier les paramètres. Sélectionnez Default si vous voulez modifier les paramètres par défaut. Ceux-ci seront utilisés pour tous les domaines dont vous n'avez pas modifié les paramètres. Si vous procédez à des modifications dans l'un des paramètres de cet onglet, vous devez cliquer sur Appliquer. Après avoir changé certains paramètres, si vous essayez de sélectionner un autre domaine sans les avoir appliqués, un message s'affiche et vous demande si vous souhaitez ou non enregistrer les modifications avant de passer à un autre domaine. Cliquez sur Oui pour les enregistrer, ou sur Non pour les ignorer.

Activer ComAgent
Lorsque cette option est activée, l'utilitaire de messagerie ComAgent est disponible pour les utilisateurs du domaine sélectionné. Ils peuvent le télécharger à partir de la page Options » ComAgent dans WorldClient. Le fichier d'installation téléchargé est automatiquement personnalisé pour chaque compte d'utilisateur afin de faciliter l'installation et la configuration.

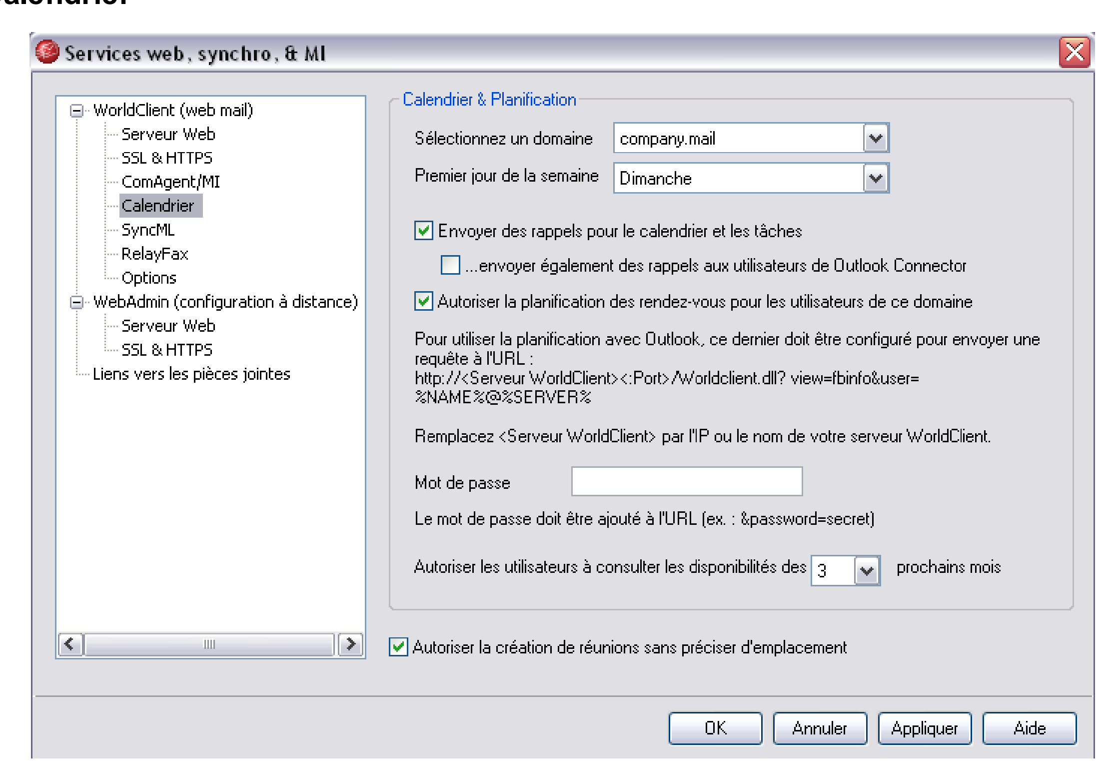
Activer la M.I.
Activez cette option si vous voulez activer le système de messagerie instantanée (M.I) de ComAgent pour les utilisateurs du domaine sélectionné.

Auditer le trafic de la M.I au niveau du serveur
Cochez cette case si vous souhaitez que tout le trafic de messagerie instantanée du domaine sélectionné soit enregistré dans le fichier `InstantMessaging.log` (situé dans le dossier `MDaemon/LOGS/`).

Inclure des membres d'autres domaines dans la liste de contacts
Cochez cette option si vous voulez que tous les utilisateurs MDaemon (quel que soit leur domaine) puissent être ajoutés dans la liste de contacts du domaine sélectionné. Désactivez cette option si vous souhaitez que seuls les utilisateurs du même domaine puissent être ajoutés dans la liste de contacts. Par exemple, si votre serveur MDaemon héberge le courrier d'exemple.com et de ma-société.com, en activant cette option pour vos utilisateurs d'exemple.com, ils peuvent ajouter des contacts des deux domaines hébergés dans leurs listes. En la désactivant, vos utilisateurs ne peuvent ajouter que des utilisateurs d'exemple.com.

Envoyer des rappels par M.I à partir de [*texte*]
Lorsqu'un rendez-vous est programmé sur le calendrier WorldClient d'un utilisateur, il est possible de définir l'envoi d'un rappel de cet événement à l'utilisateur à un certain moment. Si la messagerie instantanée est activée pour le domaine de cet utilisateur, un rappel sera envoyé dans un message instantané s'il utilise ComAgent. Utilisez cette zone de texte pour indiquer le nom que vous souhaitez voir figurer dans le champ 'De:'.

3.3.1.3.4 Calendrier



Calendrier & Planification

Sélectionnez un domaine
Choisissez dans cette liste déroulante le domaine pour lequel vous voulez modifier le calendrier. Lorsque vous modifiez un paramètre de cet onglet, vous devez cliquer sur Appliquer. Après avoir changé certains paramètres, si vous essayez de sélectionner un autre domaine sans les avoir appliqués, un message s'affiche et vous demande si vous souhaitez ou non enregistrer les modifications avant de passer à un autre domaine. Cliquez sur Oui pour les enregistrer, ou sur Non pour les ignorer.

Premier jour de la semaine
Choisissez un jour dans la liste déroulante. Le jour sélectionné apparaîtra dans les calendriers du domaine comme le premier jour de la liste.

Envoyer des rappels pour le calendrier et les tâches
Cochez cette option si vous souhaitez que WorldClient envoie aux utilisateurs des rappels pour les événements du calendrier ou les tâches par e-mail ou par ComAgent.

Envoyer également des rappels aux utilisateurs de Outlook Connector
Si l'option précédente est activée, cochez celle-ci pour envoyer également les rappels aux utilisateurs de Outlook Connector.

Options de planification

MDaemon inclut un serveur permettant de consulter directement les disponibilités des utilisateurs que l'on souhaite convier lors de la création d'un rendez-vous. Pour accéder à cette fonctionnalité, il suffit de cliquer sur Planification (lors de la création du rendez-vous dans WorldClient). Un code de couleurs indique la disponibilité de chaque participant choisi (occupé, absent du bureau, etc.). De plus en cliquant sur Recherche automatique vous obtenez la prochaine plage horaire à laquelle tous les participants seront disponibles. Une fois le rendez-vous créé, une invitation est envoyée à tous les participants, qui peuvent alors l'accepter ou la refuser.

Ce serveur est également compatible avec Microsoft Outlook. Pour cela Outlook doit être configuré pour envoyer une requête à URL du serveur. Dans Outlook 2003, les options de disponibilité se trouvent dans "Outils » Options » Options du calendrier... » Options de disponibilité..."

URL du serveur de gestion des disponibilités :

```
http://<WorldClient><:Port>/Worldclient.dll?view=fbinfo&user=%NAME
%@%SERVER%
```

Remplacez "<WorldClient>" par l'adresse IP ou le nom de serveur et <:Port> par le numéro de port (si vous n'utilisez pas le port par défaut). Exemple :

```
http://exemple.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Pour en savoir plus sur cette fonctionnalité, consultez l'aide en ligne de WorldClient.

Autoriser la planification des rendez-vous pour les utilisateurs de ce domaine
Accorde l'accès aux options de planification aux utilisateurs du domaine sélectionné précédemment.

Mot de passe
Si vous souhaitez exiger un mot de passe lorsque des utilisateurs essaient d'accéder à ce service avec Outlook, indiquez-le ici. Ce mot de passe devra être ajouté à l'URL (sous la forme : "`&password=motdepasse`") lors de la configuration d'Outlook. Exemple :

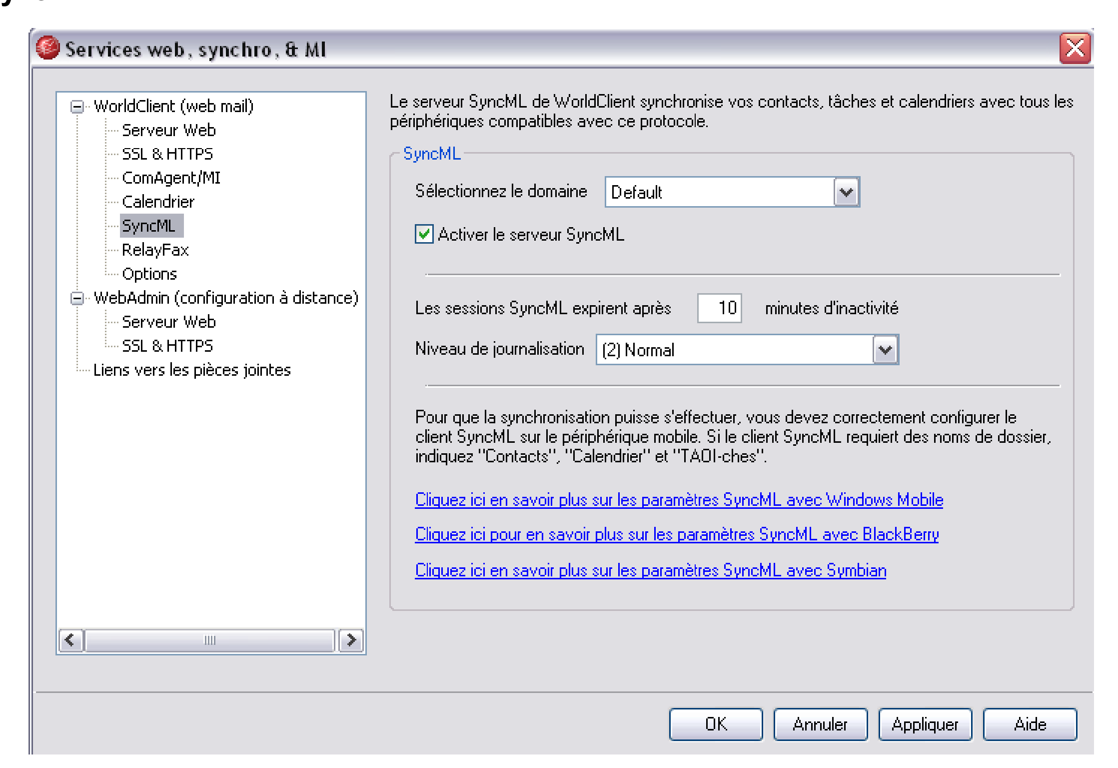
```
http://exemple.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER
%&password=motdepasse
```

Autoriser les utilisateurs à consulter les disponibilités des X prochains mois
Indiquez pour quelle période les utilisateurs peuvent consulter les disponibilités.

Options de rendez-vous

Autoriser la création de réunions sans préciser d'emplacement
Cochez cette option si vous ne souhaitez pas que les utilisateurs aient à préciser un emplacement dans le calendrier lorsqu'ils créent un rendez-vous. Décochez la case pour que toutes les rendez-vous correspondent obligatoirement à un emplacement lorsqu'ils sont programmées. Il s'agit d'un paramètre global qui ne peut pas être configuré par domaine.

3.3.1.3.5 SyncML



WorldClient inclut un serveur SyncML permettant de synchroniser vos dossiers Calendrier, Contacts, Notes et Tâches avec des périphériques compatibles SyncML. Si votre BlackBerry ou autre smartphone ne supporte pas SyncML, vous devez installer un client tiers. Exemples de clients : Funambol Sync Client, Synthesis et SyncJE. Il existe également des clients permettant de synchroniser votre calendrier avec un client de messagerie comme Microsoft Outlook. Par exemple, Funambol Sync Client est disponible pour Outlook, BlackBerry, Windows Mobile et d'autres types d'applications et appareils. Certains clients sont gratuits.

Plus d'informations sur SyncML et sa spécification sont disponibles sur le site de l'OMA (Open Mobile Alliance).

SyncML

Sélectionnez le domaine
Choisissez dans le menu déroulant le domaine pour lequel vous souhaitez activer le serveur SyncML. Configurez ensuite les options de votre choix puis cliquez sur Appliquer. Si vous sélectionnez "Default", tous les paramètres définis dans cette fenêtre seront appliqués aux nouveaux domaines ainsi qu'aux domaines existants pour lesquels les options SyncML n'ont pas été choisies.

Activer le serveur SyncML
Indique si le serveur SyncML est disponible pour le domaine sélectionné.

Les sessions SyncML expirent après X minutes d'inactivité
Durée pendant laquelle une session SyncML peut rester inactive avant d'être fermée automatiquement. Cette option est globale et s'applique à toutes les sessions quel que soit le domaine.

Niveau de journalisation
Il existe 6 niveaux différents : 1-Débogage, 2-Normal, 3-Avertissements et erreurs uniquement, 4-Erreurs uniquement, 5-Erreurs critiques uniquement et 6-Pas de journalisation. Cette option est également globale : le niveau choisi s'applique à tous les domaines.

3.3.1.3.5.1 Configuration des clients SyncML

Afin de bénéficier du serveur SyncML de WorldClient, les clients doivent être configurés pour se connecter à l'URL suivante :

```
http://<Serveur WorldClient><:port>/MDSyncML.dll
```

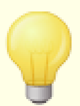
Exemples :

```
http://mail.exemple.com:3000/MDSyncML.dll
http://www.example.com/MDSyncML.dll
```

Si le client requiert des noms de dossiers, indiquez Contacts, Calendrier et T&AOI-ches (cela est dû à un problème de codage des caractères spéciaux dans les noms de dossiers).

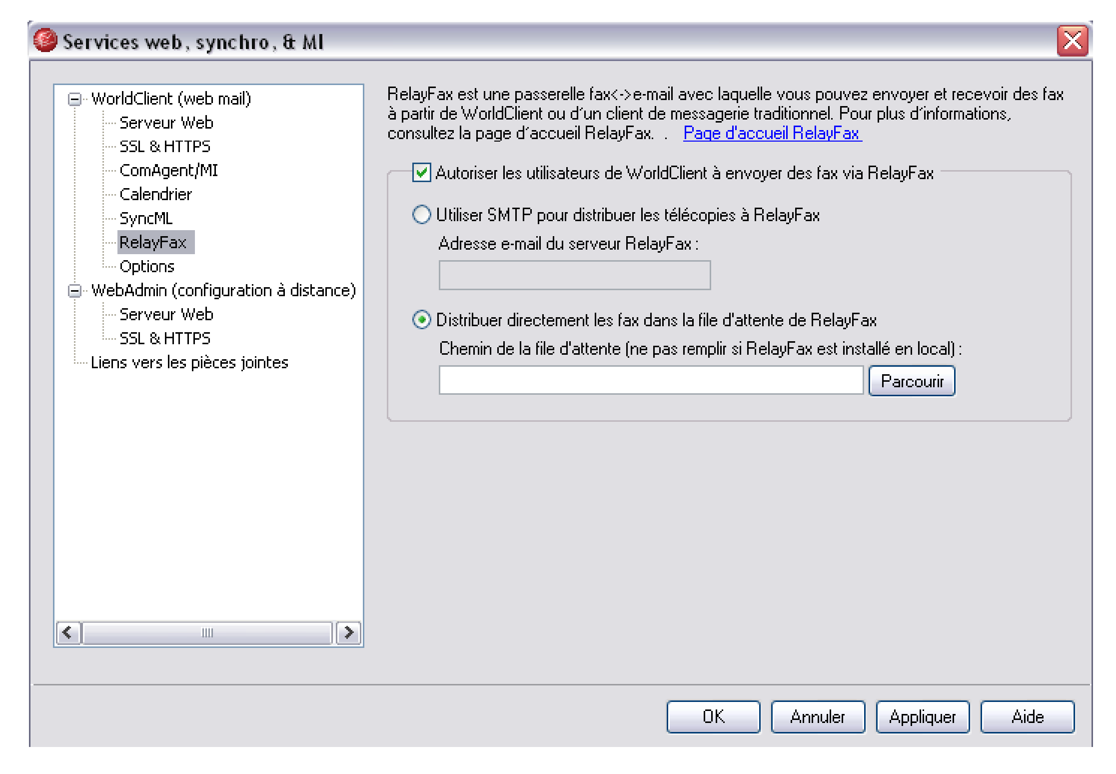
Le serveur accepte les formats suivants pour les noms de dossier :

`contacts`
`/contacts`
`./contacts`
`contacts/perso` (s'il y a un sous-dossier appelé "perso")
`contacts.imap\perso.imap`



Afin d'effectuer une synchronisation avec SyncML, l'utilisateur doit s'être connecté au moins une fois à WorldClient.

3.3.1.3.6 RelayFax



Le serveur RelayFax de Alt-N Technologies est une passerelle messagerie/fax et fax/messagerie qui peut être intégrée totalement à WorldClient pour fournir des services de fax à vos utilisateurs. Lorsque cette fonctionnalité est activée, les utilisateurs de WorldClient ont accès à plusieurs fonctions qui leur permettent de rédiger et d'envoyer des fax depuis WorldClient. Pour plus d'informations concernant RelayFax, consultez la partie concernant RelayFax du site www.altn.com.

Options d'intégration de RelayFax

Autoriser les utilisateurs WorldClient à envoyer des fax avec RelayFax
Activez cette option pour intégrer RelayFax à WorldClient. Dans ce cas, l'option Composer Fax et d'autres fonctions liées au fax apparaissent dans les pages de

WorldClient.

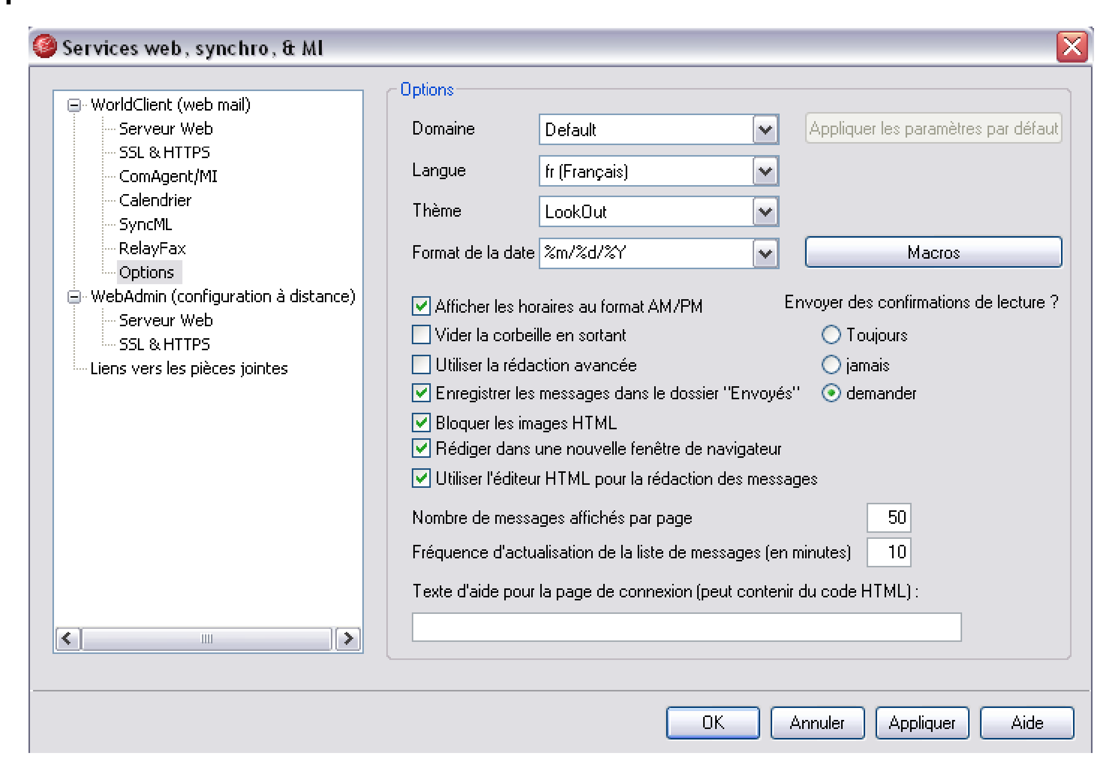
Utiliser SMTP pour distribuer les télécopies à RelayFax
RelayFax surveille une boîte aux lettres spécifique pour les messages entrants à faxer. Lorsque cette option est activée, MDaemon utilise le processus normal de distribution de courrier SMTP pour envoyer ces messages à l'adresse de cette boîte aux lettres. Cette option est utile lorsque RelayFax surveille une boîte aux lettres située ailleurs que sur votre LAN. Si RelayFax est situé sur votre LAN, MDaemon peut distribuer ces messages directement dans la file de messages de RelayFax, sans qu'ils ne passent par le processus de distribution SMTP. Pour des informations complémentaires sur cette méthode, voir *Distribuer les fax directement dans la file d'attente de RelayFax* ci-dessous.

Adresse e-mail du serveur RelayFax
Indiquez l'adresse à laquelle vous souhaitez que les messages à faxer soient distribués. Cette valeur doit correspondre à l'adresse configurée sur laquelle RelayFax surveille l'arrivée des messages.

Distribuer les fax directement dans la file d'attente de RelayFax
Si RelayFax est situé sur votre LAN, vous pouvez choisir cette méthode plutôt que le processus SMTP pour distribuer les messages à faxer. Lorsque MDaemon reçoit un message destiné à RelayFax, il le placera directement dans la file d'entrée RelayFax au lieu de le distribuer par SMTP.

Chemin de la file d'attente
Si RelayFax se situe sur le même poste que celui sur lequel MDaemon fonctionne, vous pouvez laisser ce champ vide. Sinon, vous devez indiquer un chemin réseau vers le répertoire \app\ de RelayFax.

3.3.1.3.7 Options



Les paramètres de cet onglet sont spécifiques à chaque domaine. La majorité de ces options concernent le comportement du serveur WorldClient au niveau du client plutôt que son comportement global et sa configuration.

Options

Domaine

Utilisez cette liste déroulante pour choisir le domaine dont vous souhaitez modifier les paramètres. Sélectionnez Default si vous voulez modifier les paramètres par défaut. Ceux-ci seront utilisés pour tous les domaines dont vous n'avez pas modifié les paramètres. Si vous procédez à des modifications dans l'un des paramètres de cet onglet, vous devez cliquer sur Appliquer. Après avoir changé certains paramètres, si vous essayez de sélectionner un autre domaine sans les avoir appliqués, un message s'affiche et vous demande si vous souhaitez ou non enregistrer les modifications avant de passer à un autre domaine. Cliquez sur Oui pour les enregistrer, ou sur Non pour les ignorer.

Appliquer les paramètres par défaut

Cliquez sur ce bouton pour appliquer les paramètres par défaut au domaine sélectionné.

Langue (MDaemon PRO seulement)

Utilisez cette liste déroulante pour choisir la langue dans laquelle s'affiche l'interface de WorldClient lorsque vos utilisateurs se connectent pour la première fois au domaine sélectionné. Les utilisateurs peuvent modifier leur paramètre personnel de langue sur la page de connexion à WorldClient, ou via l'option située dans l'onglet

Options » Personnaliser de WorldClient.

Thème (MDaemon PRO only)
Utilisez cette liste déroulante pour indiquer le thème WorldClient par défaut à utiliser pour l'interface client lorsque les utilisateurs se connectent pour la première fois au domaine indiqué. Les utilisateurs peuvent personnaliser la configuration de ce thème depuis Options » Personnaliser dans WorldClient.

Format de la date
Choisissez le format des dates pour le domaine sélectionné dans cette liste déroulante. Cliquez sur le bouton Macros pour afficher une liste de codes de macros qui peuvent être utilisés dans cette zone de texte. Les macros pouvant être utilisées dans cette commande sont les suivantes :

%A—Nom entier jour

%B—Nom entier du mois

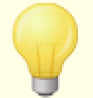
%d—Jour du mois (01 – 31)

%m—Mois (01 – 12)

%y—Année sur deux chiffres

%Y—Année sur quatre chiffres

Par exemple, "%m/%d/%Y" s'affiche dans WorldClient sous la forme "12/25/2002".



Ce paramètre fonctionne par domaine. Les utilisateurs individuels ne peuvent pas modifier le format de date utilisé pour leurs comptes.

Macros
Cliquez sur ce bouton pour afficher la liste des codes de macros qui peuvent être utilisés dans le Format de date.

Afficher les horaires au format AM/PM
Décochez cette option si vous souhaitez afficher l'heure au format 24h pour le domaine sélectionné. Les utilisateurs peuvent modifier ce paramètre en cliquant sur Options » Calendrier dans WorldClient.

Vider la corbeille en sortant
Avec cette option, la corbeille de l'utilisateur est vidée lorsqu'il quitte WorldClient. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Personnaliser dans WorldClient.

Utiliser la rédaction avancée
Cliquez sur cette option pour que, par défaut, la fenêtre Mode avancé s'ouvre plutôt que la fenêtre normale de rédaction pour les utilisateurs de ce domaine. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Rédaction dans WorldClient.

Enregistrer les messages dans le dossier 'Envoyés'
Sélectionnez cette option si vous souhaitez qu'une copie de chaque message envoyé soit enregistrée dans le dossier Envoyés de la boîte aux lettres. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Rédaction dans WorldClient.

Rédiger dans une nouvelle fenêtre de navigateur
Activez cette option si vous voulez qu'une fenêtre de navigateur séparée s'ouvre pour rédiger des messages au lieu de passer simplement de la fenêtre principale à l'écran de rédaction. Décochez cette case si vous ne voulez pas qu'une nouvelle fenêtre s'ouvre. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Rédaction dans WorldClient.

Utiliser l'éditeur HTML pour la rédaction des messages
Cette option affiche par défaut l'éditeur html lors de la rédaction d'un nouveau message. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Rédaction dans WorldClient.

Envoyer des confirmations de lecture ?
Indiquez ici comment vous souhaitez que WorldClient réponde aux messages contenant des requêtes de confirmation de lecture.

toujours
Si vous sélectionnez cette option, une notification indiquant que le message a été ouvert est envoyée à l'expéditeur. Cela s'effectue de façon transparente pour votre utilisateur : rien ne lui indique que la confirmation a été demandée ou renvoyée.

jamais
Sélectionnez cette option si vous souhaitez ne jamais répondre aux confirmations de lecture.

demander
Sélectionnez cette option si vous souhaitez laisser choisir l'utilisateur d'envoyer ou non la confirmation lorsqu'un message la demande.

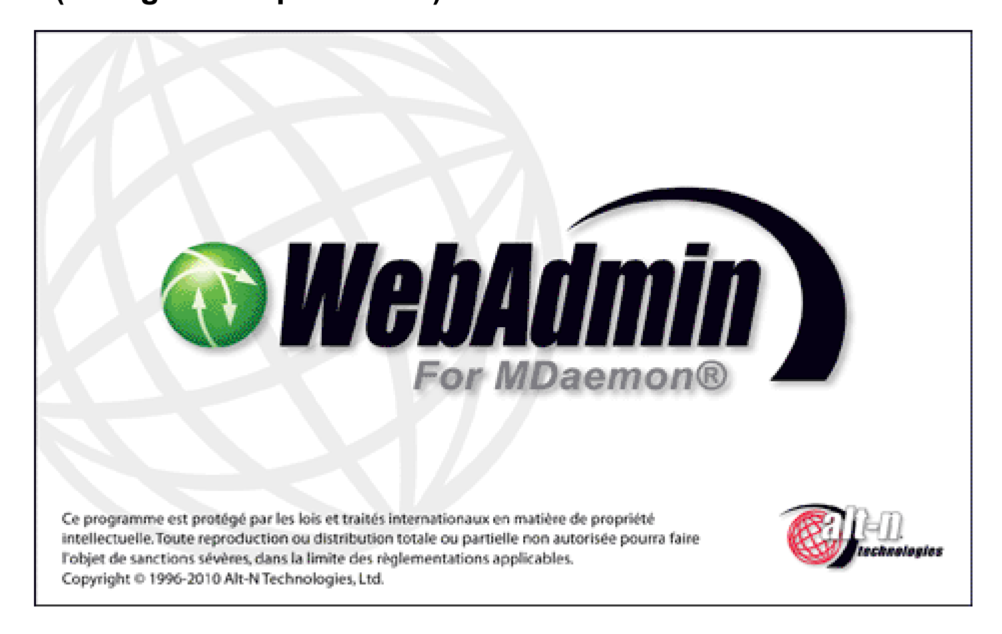
Nombre de messages affichés par page
Il s'agit du nombre de messages affichés sur chaque page de la liste de messages pour chacun des dossiers de courrrier. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Personnaliser dans WorldClient.

Fréquence d'actualisation de la liste de messages (en minutes)
Il s'agit du nombre de minutes pendant lequel WorldClient attend avant d'actualiser automatiquement la liste des messages. Les utilisateurs individuels peuvent modifier ce paramètre en cliquant sur Options » Personnaliser dans WorldClient.

Texte d'aide pour la page de connexion (peut contenir du code HTML)
Le texte (brut ou HTML) indiqué dans ce champ est affiché sur la page de connexion à WorldClient lorsqu'un utilisateur rencontre un problème. Ce texte s'affiche en-

dessous du message d'erreur par défaut : "*Identifiant incorrect, veuillez réessayer. Si vous avez besoin d'assistance, veuillez contacter votre administrateur.*" Vous pouvez ainsi indiquer aux utilisateurs des liens spécifiques ou bien le nom de la personne à contacter par exemple.

3.3.2 WebAdmin (configuration par le web)



WebAdmin est une application conçue pour administrer à distance, via le Web, des logiciels de l'éditeur Alt-N Technologies. WebAdmin est intégré dans MDaemon et permet d'administrer aussi bien MDaemon que son serveur webmail intégré WorldClient®.

WebAdmin est une application serveur qui s'exécute en arrière-plan sur le même poste que le logiciel de Alt-N Technologies à administrer. Pour accéder à WebAdmin, il suffit d'ouvrir le navigateur et de saisir l'adresse et le port de l'application. (www. monwebadmin.com:1000, par exemple). Après avoir entré vos identifiants de connexion, vous accédez à différents paramètres et options de MDaemon et de ses modules. La sélection de paramètres disponibles, et leur quantité, dépendent du niveau d'accès accordé. Il existe trois niveaux d'accès attribués aux utilisateurs WebAdmin : accès administrateur système (ou global), accès administrateur de domaine, ou accès utilisateur.

Administrateur global —Ces administrateurs ont un droit d'accès global, activé pour les paramètres de leur compte dans MDaemon. Cet accès global signifie que l'utilisateur autorisé peut visualiser et configurer tous les paramètres et options accessibles via WebAdmin. Les administrateurs globaux peuvent ajouter, modifier, et supprimer des utilisateurs, des domaines et des listes de diffusion. Ils ont également la possibilité de modifier des fichiers INI, désigner d'autres utilisateurs en tant qu'administrateurs de domaine, gérer des mots de passe etc. ; ils possèdent un contrôle administratif total.

Administrateur de domaine —Semblables aux administrateurs globaux, les administrateurs de domaine possèdent un contrôle total sur tous les utilisateurs

et paramètres des logiciels. Ce contrôle administratif est cependant limité à un ou plusieurs domaines pour lesquels ils ont été autorisés. Les administrateurs de domaine et les domaines qu'ils contrôlent sont sélectionnés à partir de WebAdmin, par un administrateur système ou un autre administrateur de domaine, possédant déjà un droit d'accès à ces domaines.

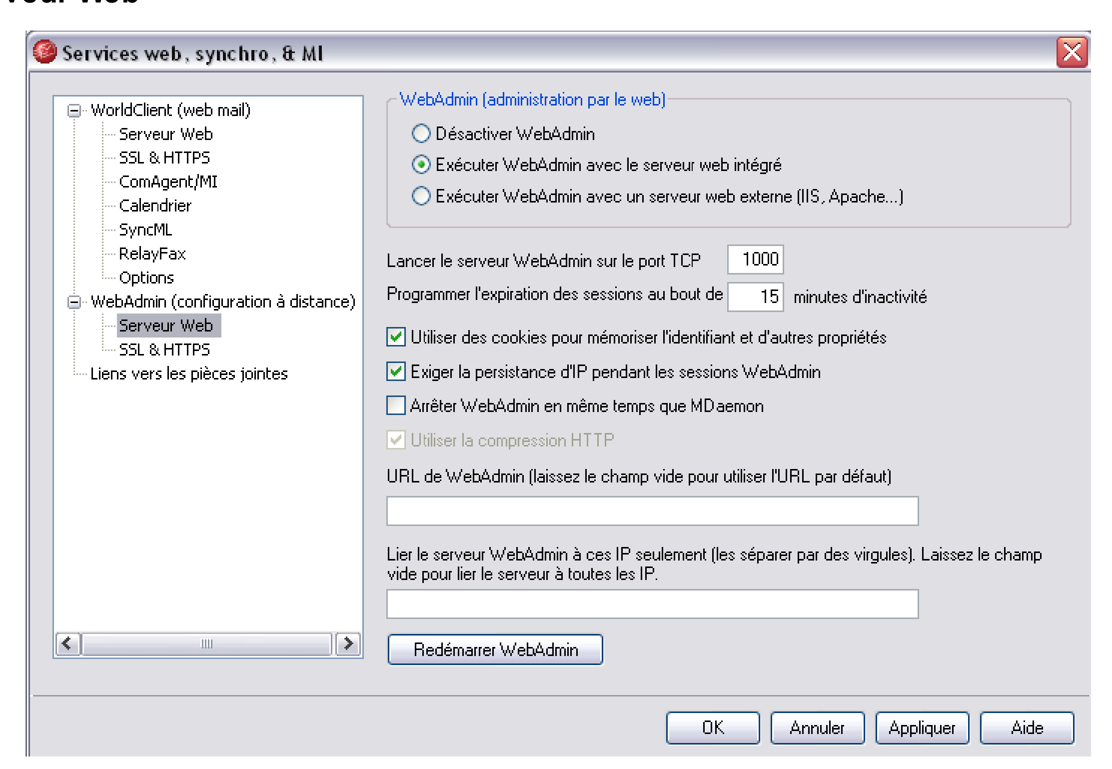
Utilisateur —L'accès utilisateur est le niveau d'accès le plus bas. Les utilisateurs MDaemon peuvent, par exemple, se connecter à WebAdmin pour visualiser les paramètres de leur propre compte et en modifier les entrées MultiPOP, filtres de courrier, répondeurs automatiques etc. La sélection et la quantité de paramètres pouvant être modifiés, dépendent des droits attribués sur les paramètres de compte de chaque utilisateur.

Tout utilisateur possédant les droits nécessaires peut accéder à WebAdmin en cliquant sur Options > Paramètres avancés dans WorldClient. WebAdmin s'ouvre alors dans une nouvelle fenêtre (ou un nouvel onglet) du navigateur.

Voir également :

WebAdmin » Serveur Web 130
WebAdmin » HTTPS 132
Paramètres par défaut des nouveaux comptes » Accès web 335
Éditeur de compte » WorldClient & WebAdmin 304
Exécuter WebAdmin sous IIS 135

3.3.2.1 Serveur Web



WebAdmin (configuration à distance)

Désactiver WebAdmin
Vous pouvez également activer/désactiver WebAdmin dans le menu Fichier ou dans l'onglet Statistiques de l'interface principale.

Exécuter WebAdmin avec le serveur web intégré
Cochez cette option pour exécuter WebAdmin avec le serveur web intégré de MDaemon.

Exécuter WebAdmin avec un serveur web externe (IIS, Apache...)
Cochez cette option si vous souhaitez exécuter WebAdmin sous IIS ou tout autre serveur web. Cela bloque l'accès à certaines options qui pourraient entraîner un conflit avec votre serveur.

Pour plus d'informations, voir Exécuter WebAdmin sous IIS 135.

Lancer le serveur WebAdmin sur le port TCP ...
Détermine le port que WebAdmin écoute pour se connecter à partir de votre navigateur. Par défaut : 1000.

Programmer l'expiration des sessions au bout de x minutes d'inactivité
Détermine au bout de combien de temps WebAdmin ferme une session lorsqu'elle est inactive.

Utiliser des cookies pour mémoriser l'identifiant et d'autres propriétés
Sélectionnez cette option pour que WebAdmin stocke l'identifiant et d'autres propriétés de l'utilisateur dans un cookie sur son ordinateur local. Ainsi, les utilisateurs disposent d'un profil de connexion personnalisé. Cela nécessite toutefois que les cookies soit acceptés par le navigateur.

Exiger la persistance d'IP pendant les sessions WebAdmin
Pour plus de sécurité, vous pouvez activer cette option afin que WebAdmin restreigne chaque session utilisateur à l'adresse IP à partir de laquelle l'utilisateur se connecte au début de la session. Ainsi, personne ne peut "voler" la session de l'utilisateur puisque la persistance d'IP est requise. Cette configuration est sécurisée mais elle peut poser des problèmes aux utilisateurs qui utilisent un serveur proxy ou un compte d'accès par ligne commutée qui attribue et modifie de façon dynamique les adresses IP.

Arrêter WebAdmin en même temps que MDaemon
Cochez cette option si vous souhaitez que WebAdmin soit arrêté en même temps que MDaemon. Sinon, il sera toujours exécuté en arrière-plan.

URL de WebAdmin
URL utilisée par WorldClient lorsqu'un utilisateur clique sur le lien Paramètres avancés pour accéder à WebAdmin. Si WebAdmin fonctionne avec le serveur intégré, il n'est pas nécessaire de remplir ce champ. Par contre, avec un autre serveur, vous devez indiquer l'URL choisie pour WebAdmin.

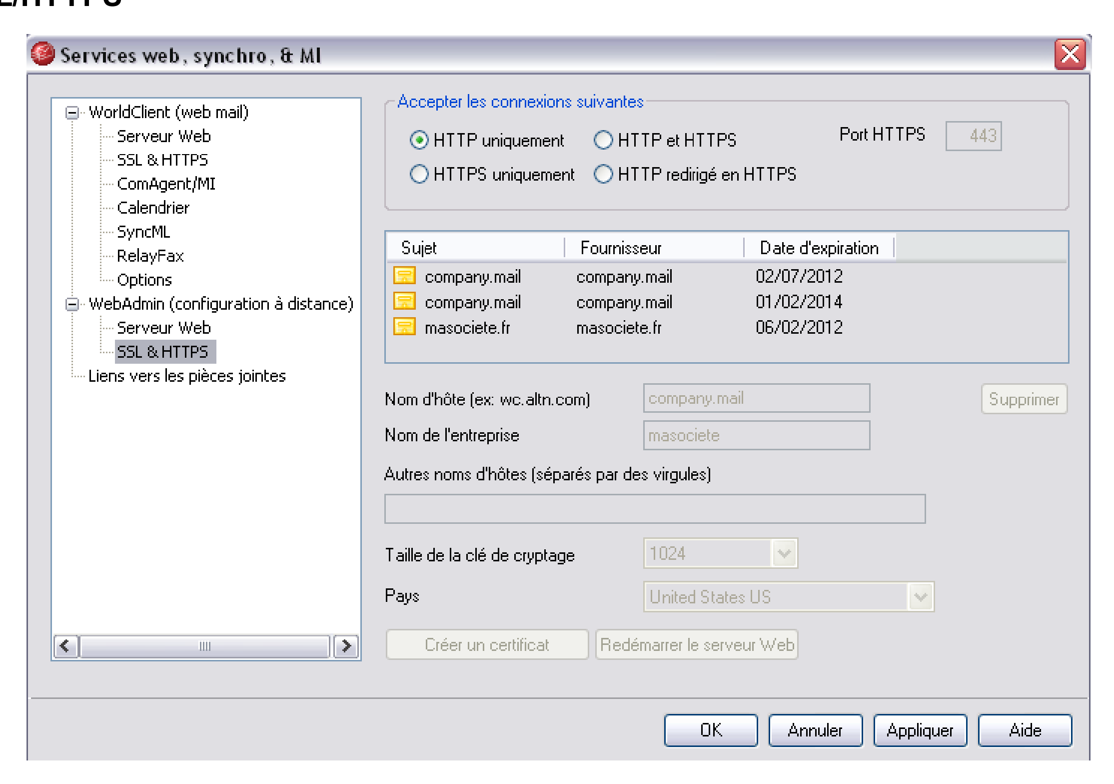
Lier le serveur WebAdmin à ces IP seulement
Si vous souhaitez limiter le serveur WebAdmin à certaines adresses IP, indiquez-les dans ce champ et séparez-les par des virgules. Lorsque ce champ n'est pas rempli, WebAdmin accepte toutes les adresses spécifiées pour le domaine principal et les domaines supplémentaires.

Redémarrer WebAdmin (nécessaire en cas de changement de port ou de valeur IIS)
Cliquez sur ce bouton pour redémarrer le serveur WebAdmin. Remarque : lorsque vous modifiez le numéro de port de WebAdmin, vous devez redémarrer WebAdmin afin que la nouvelle configuration soit prise en compte.

Voir également :

WebAdmin (configuration à distance) 129
WebAdmin » HTTPS 132
Exécuter WebAdmin sous IIS 135
Modèle de compte » WorldClient et WebAdmin 335
Éditeur de compte » WorldClient et WebAdmin 304

3.3.2.2 SSL/HTTPS

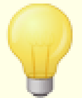


Le serveur Web de MDaemon supporte le protocole SSL (Secure Sockets Layer). Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il fournit l'authentification du serveur, le cryptage de données, et l'authentification facultative

du client pour la connexion TCP/IP. De plus, dans la mesure où SSL est intégré aux principaux navigateurs actuels, en installant simplement un certificat numérique valide sur votre serveur, les fonctions SSL du client qui se connecte sont activées.

Les options relatives à l'activation et à la configuration de WebAdmin pour qu'il utilise le protocole SSL/HTTPS, se trouvent dans la boîte de dialogue SSL & HTTPS (Configuration » Services Web, Synchro et MI » WebAdmin". Pour plus de commodité, ces options sont également accessibles dans la boîte de dialogue "Sécurité » Paramètres de sécurité » SSL & TLS » WebAdmin".

Pour en savoir plus sur ce protocole, voir : **SSL & certificats** 271



Les éléments de cette boîte de dialogue s'appliquent uniquement lorsque WebAdmin utilise le serveur web intégré de MDaemon. Si vous avez configuré WebAdmin pour fonctionner un autre serveur, ces options ne seront alors pas utilisées—le support SSL/HTTPS doit être configuré dans le serveur choisi.

Accepter les connexions suivantes

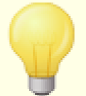
HTTP uniquement
Sélectionnez cette option si vous ne souhaitez pas autoriser les connexions HTTPS à WebAdmin. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS
Cette option accepte le support SSL pour WebAdmin, mais les utilisateurs ne sont pas obligés d'employer des connexions HTTPS. Dans ce cas WebAdmin écoute les connexions HTTPS sur le port indiqué ci-dessous, mais il répond également aux connexions HTTP normales.

HTTPS uniquement
Avec cette option, il est obligatoire d'utiliser une connexion HTTPS pour se connecter à WebAdmin. Les requêtes HTTP ne sont pas acceptées.

HTTP redirigé en HTTPS
Sélectionnez cette option pour rediriger toutes les connexions HTTP sur le port HTTPS.

Port HTTPS
Il s'agit du port TCP que WebAdmin écoutera pour les connexions SSL. Le port SSL par défaut est le port 443. Si le port SSL par défaut est utilisé, vous n'aurez pas à inclure le numéro du port dans l'URL de WebAdmin lors de la connexion par HTTPS (https://exemple.com est équivalent à https://exemple.com:443).



Le port HTTPS n'est pas le même que celui indiqué dans l'onglet Serveur Web 111 des propriétés de WebAdmin. Si vous autorisez toujours les connexions HTTP vers WebAdmin, ces connexions devront alors utiliser cet autre port pour pouvoir

être effectuées correctement. Les connexions HTTPS doivent utiliser le port HTTPS.

Certificats

Cette boîte présente vos certificats SSL. Cliquez une fois sur un certificat pour le sélectionner et l'utiliser. Double-cliquez sur un certificat pour visualiser les détails le concernant dans la boîte de dialogue Certificat.



MDaemon ne permet pas à WorldClient d'utiliser plusieurs certificats. Tous les domaines de WorldClient doivent donc partager un même certificat. Si vous avez plusieurs domaines WorldClient, entrez leur nom (et celui des autres domaines auxquels vous souhaitez autoriser l'accès à WorldClient) dans le champ *Autres noms d'hôtes*, situé en dessous.

Supprimer
Sélectionnez un certificat dans la liste puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous voulez vraiment supprimer ce certificat.

Nom d'hôte
Saisissez le nom de l'hôte auquel vos utilisateurs se connecteront (par exemple, "courrier.exemple.com").

Nom de l'entreprise
Saisissez le nom de l'organisme ou de la société "propriétaire" du certificat.

Autres noms d'hôtes (séparés par des virgules)
Actuellement, MDaemon ne permet pas à chaque domaine WebAdmin de posséder son propre certificat : ils doivent donc tous partager le même. Saisissez dans ce champ, en les séparant par des virgules, le nom des autres domaines auxquels les utilisateurs se connecteront et auxquels le certificat s'appliquera. Les caractères jokers sont acceptés. Ainsi, "`*.exemple.com`" s'appliquera à tous les sous-domaines d'`exemple.com` (par exemple, "`wc.exemple.com`", " `mail.exemple.com`", etc).

Taille de la clé de cryptage
Choisissez la longueur, en bits, de la clé de cryptage pour ce certificat. Plus la clé de cryptage est longue, plus le transfert des données est sécurisé. Veuillez noter que toutes les applications ne supportent pas toutes des clés de plus de 512 bits.

Pays
Indiquez dans quel pays se trouve votre serveur.

Créer un certificat
Lorsque vous avez saisi toutes les informations requises dans les champs

précédents, cliquez sur ce bouton pour créer votre certificat.

Redémarrer le serveur Web
Cliquez sur ce bouton pour redémarrer WorldClient. Il doit être relancé avant l'utilisation des nouveaux certificats.

Pour en savoir plus sur SSL et les certificats, voir :

Exécuter WebAdmin sous IIS 135
SSL et certificats 271
Création et utilisation de certificats SSL 281

Pour en savoir plus sur WebAdmin, voir :

Configuration à distance 129
WebAdmin » Serveur web 130
Modèle de compte » WorldClient et WebAdmin 335
Éditeur de compte » WorldClient et WebAdmin 304

3.3.2.3 Exécuter WebAdmin sous IIS

WebAdmin n'a pas besoin d'IIS pour être opérationnel car il est pourvu d'un serveur intégré. Cependant, il assure le support de ce serveur et peut donc fonctionner en tant que DLL ISAPI.

Configuration de WebAdmin sous IIS 5 :

1. Arrêtez WebAdmin (depuis le menu Fichier ou l'onglet Statistiques de l'interface principale).

2. Ouvrez le programme de gestion d'IIS (Démarrer » Paramètres » Panneau de configuration » Outils d'administration » Gestionnaire des services Internet).

3. Effectuez un clic droit sur Site Web par défaut puis sélectionnez **Nouveau → Répertoire virtuel**.

4. Suivez les différentes étapes de la création du répertoire. Les noms et emplacements des données ne figurent qu'à titre d'exemple et varient en fonction de la configuration de MDaemon et de l'emplacement de WebAdmin.

   a. Alias : "WebAdmin". Cliquez sur Suivant.

   b. Répertoire : "c:\mdaemon\webadmin\templates". Cliquez sur Suivant.

   c. Cliquez sur Suivant.

   d. Cliquez sur Terminer.

5. Configurez l'option **Autorisations d'exécution** sur **Scripts seulement**.

6. Configurez l'option **Protection d'application** sur **Basse (Processus IIS)**.

7. Cliquez sur le bouton **Configuration**.

8. Dans l'onglet **Mappage d'application**, cliquez sur **Ajouter**.

9. Indiquez : "c:\mdaemon\webadmin\templates\WebAdmin.dll" dans le champ **Exécutable**. Remarque : Le nom du chemin ne doit pas contenir d'espaces. S'il en contient, il doit être converti au format 8.3. (s'affiche à l'aide de la commande dir / x.)

10. Indiquez : ".wdm" dans le champ **Extension** et cochez **Tous les verbes**.

11. Cochez l'option **Moteur de script**.

12. Cliquez sur **OK**.

13. Vous pouvez éventuellement supprimer les autres mappages avant de cliquer à nouveau sur **OK**.

14. Dans l'onglet **Documents** ajoutez le document par défaut : login.wdm et supprimez toutes les autres entrées de la liste.

15. Dans MDaemon, cliquez sur Configuration » Services Web, synchro et MI » WebAdmin… puis cochez **Activer le serveur WebAdmin** et **Exécuter WebAdmin sous IIS**.

16. Indiquez "/WebAdmin/login.wdm" dans le champ **URL de WebAdmin**.

17. Cliquez sur **OK**.

Configuration de WebAdmin sous IIS 6 :

Créer un pool d'applications pour WebAdmin :

1. Arrêtez WebAdmin (depuis le menu Fichier ou l'onglet Statistiques de l'interface principale).

2. Ouvrez le programme de gestion d'IIS (Démarrer » Paramètres » Panneau de configuration » Outils d'administration » Gestionnaire des services Internet).

3. Effectuez un clic droit sur **Pools d'application**.

4. Cliquez sur Nouveau » Pool d'application.

5. Indiquez "Alt-N" dans le champ ID du pool d'applications et cliquez sur **OK**.

6. Effectuez un clic droit sur Alt-N.

7. Cliquez sur **Propriétés**.

8. Cliquez sur l'onglet **Performances**.

9. Décochez les options **Arrêter les processus de travail après une inactivité de** et **Limiter la file d'attente de demandes du noyau**.

10. Cliquez sur l'onglet **Identité**.

11. Dans le menu déroulant **Prédéfini**, sélectionnez **Système local**.

12. Cliquez sur **OK**.

Créer un répertoire virtuel pour WebAdmin :

1. Ouvrez le programme de gestion d'IIS (Démarrer » Paramètres » Panneau de configuration » Outils d'administration » Gestionnaire des services Internet).

2. Effectuez un clic droit sur votre site et sélectionnez **Nouveau** » **Répertoire virtuel**.

3. Attribuez-lui un alias (par exemple : WebAdmin).

4. Indiquez le chemin du répertoire des modèles de WebAdmin, par exemple, "C:\Program Files\Alt-N Technologies\WebAdmin\Templates".

5. Cochez les options **Lecture** et **Exécuter les scripts**.

6. Une fois la création terminée, effectuez un clic droit sur le répertoire virtuel que vous venez de créer.

7. Sélectionnez **Propriétés**.

8. Dans l'onglet **Répertoire de base** indiquez le pool d'applications Alt-N.

9. Cliquez sur **Configuration**.

10. Cliquez sur **Ajouter** afin d'inclure une extension ISAPI.

11. Indiquez le chemin du fichier WebAdmin.dll dans le champ **Exécutable**. Par exemple, "C:\Program Files\Alt-N Technologies\WebAdmin\Templates/WebAdmin.dll".

12. Dans le champ **Extension**, indiquez : ".wdm"

13. Cochez les options **Moteur de script** et **Vérifier si le fichier existe**.

14. Cliquez sur **OK**.

15. Vous pouvez éventuellement supprimer les autres mappages avant de cliquer à nouveau sur **OK**.

16. Cliquez sur l'onglet **Documents**.

17. Assurez-vous que l'option **Activer le document par défaut** soit cochée.

18. Vérifiez que "login.wdm" soit la seule entrée de la liste.

19. Cliquez sur **OK** et fermez la fenêtre.

Ajouter .WDM à la liste des extensions de service Web autorisées :

1. Cliquez sur **Extensions du service Web** (dans la console MMC pour IIS).

2. Cliquez sur **Ajouter une extension de service Web**.

3. Indiquez "WebAdmin" dans le champ **Nom d'extension**.

4. Cliquez sur **Ajouter** puis indiquez le chemin d'accès pour l'extension ISAPI de WebAdmin. Par ex. : C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll.

5. Cochez l'option **Définir le statut de l'extension** à **Autorisée**.

6. Cliquez sur **OK**.

7. Dans MDaemon, cliquez sur Configuration » Services Web, synchro et MI » WebAdmin... puis cochez **Activer le serveur WebAdmin** et **Exécuter WebAdmin sous IIS**.

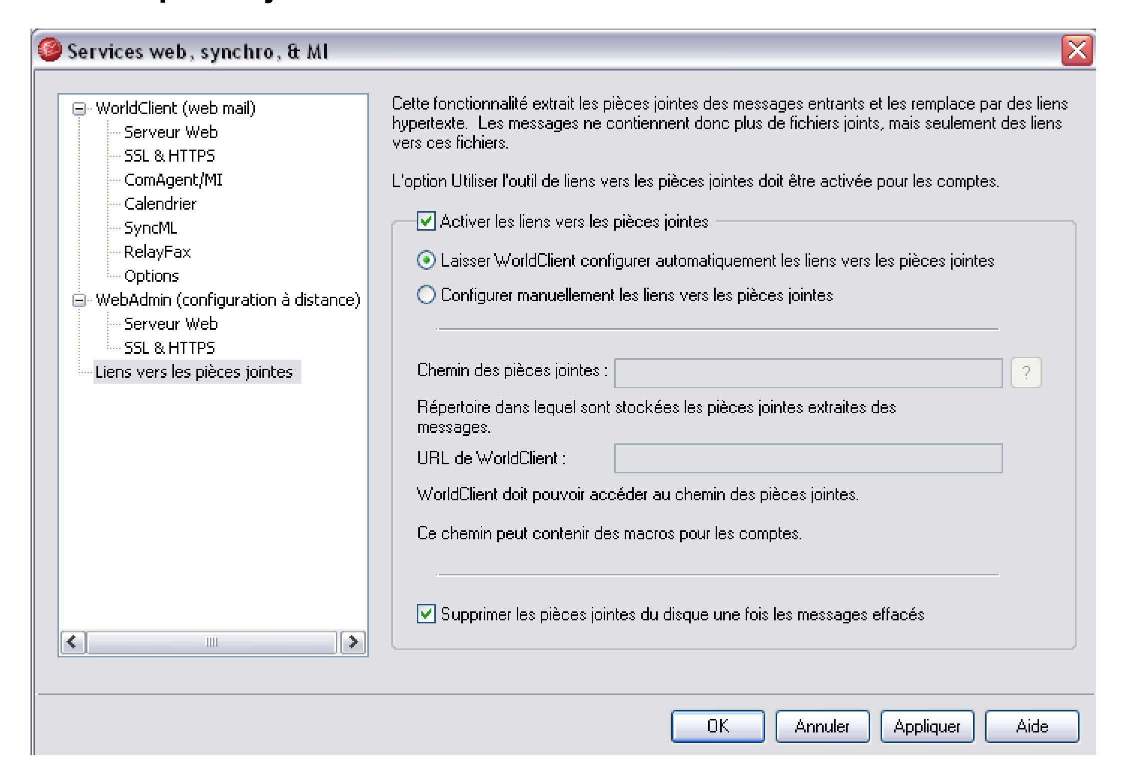
8. Indiquez "/WebAdmin/login.wdm" dans le champ **URL de WebAdmin**.

9. Cliquez sur **OK**.

Pour en savoir plus sur WebAdmin, voir :

Configuration à distance 129
WebAdmin » Serveur web 130
WebAdmin » HTTPS 132
Modèle de compte » WorldClient et WebAdmin 335
Éditeur de compte » WorldClient et WebAdmin 304

3.3.3 Liens vers les pièces jointes



Avec cette fonctionnalité, MDaemon supprime automatiquement les pièces jointes des messages entrants, les stocke dans un endroit précis, et les remplace par des liens hypertextes. Les utilisateurs n'ont plus alors qu'à cliquer sur les liens pour récupérer leurs fichiers. Cette fonction accélère significativement le traitement du courrier lorsque vos utilisateurs retirent leurs messages ou synchronisent leurs dossiers de courrier, puisqu'il ne contient pas de pièces jointes volumineuses. En outre, elle offre plus de sécurité car les pièces jointes sont centralisées, contrôlées par l'administrateur, et non téléchargées directement vers les clients de messagerie où elles pourraient être exécutées automatiquement.

Si vous sélectionnez l'option "*Laisser WorldClient configurer automatiquement les liens vers les pièces jointes*", tout s'effectue automatiquement. Si vous préférez les configurer manuellement, vous pouvez choisir l'emplacement de stockage des fichiers et utiliser des macros. Pour que les liens vers les pièces jointes fonctionnent, ils doivent être activés ici ainsi que dans l'onglet Courrier et pièces jointes 303 de l'Éditeur de compte pour tous les comptes qui les utilisent. Enfin, les URL placées dans les messages ne contiennent plus des chemins complets. Un GUID est généré et utilisé pour lier une URL à un fichier sur le disque. Les liens des GUID sont stockés dans le fichier `AttachmentLinking.dat`.

Activer les liens vers les pièces jointes

Cette option active les liens vers les pièces jointes pour les comptes configurés pour les utiliser dans l'onglet Courrier et pièces jointes 303 de l'Éditeur de compte. Si vous cochez cette case, un message vous demande si vous souhaitez activer les liens vers les pièces jointes pour tous les comptes. Si vous cliquez sur "Oui", cette fonctionnalité est activée pour tous les comptes existants ainsi que dans le Modèle de compte 330. Si vous cliquez sur "Non", la fonctionnalité est activée, mais chaque

compte doit être configuré manuellement pour l'utiliser. Lorsque cette option est activée le serveur WorldClient doit rester actif.

Laisser WorldClient configurer automatiquement les liens vers les pièces jointes
Option par défaut. Avec cette option, tout s'effectue automatiquement et les fichiers extraits sont stockés dans "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\".

Configurer manuellement les liens vers les pièces jointes
Sélectionnez cette option si vous souhaitez choisir le dossier dans lequel seront stockées les pièces jointes. Dans ce cas, vous devez désigner le chemin des pièces jointes et l'URL de WorldClient (les valeurs par défaut conviennent dans la plupart des cas).

Chemin des pièces jointes
Saisissez dans cette zone de texte le répertoire dans lequel vous souhaitez stocker les fichiers joints extraits. Vous pouvez utiliser un chemin statique ou bien utiliser des macros de modèles 333 et de scripts 343. Par exemple, "$ROOTDIR$\Fichiers\$DOMAIN$\" crée un sous-dossier pour le domaine auquel l'utilisateur appartient, dans le dossier "Fichiers" se trouvant à la racine de MDaemon (par défaut : C:\MDaemon\). Ainsi, pour "frank@exemple.com" les pièces jointes seraient stockées dans, "C:\MDaemon\Fichiers\exemple.com\." Vous pouvez également utiliser la macro "$MAILBOX$" pour ajouter un sous-dossier. Dans ce cas, le chemin serait : "C:\MDaemon\Fichiers\exemple.com\Frank\."

URL de WorldClient
Indiquez ici l'URL de WorldClient (ex. : "http://mail.exemple.com:3000/WorldClient.dll"). MDaemon utilise cette url pour insérer les liens vers les pièces jointes dans les messages.

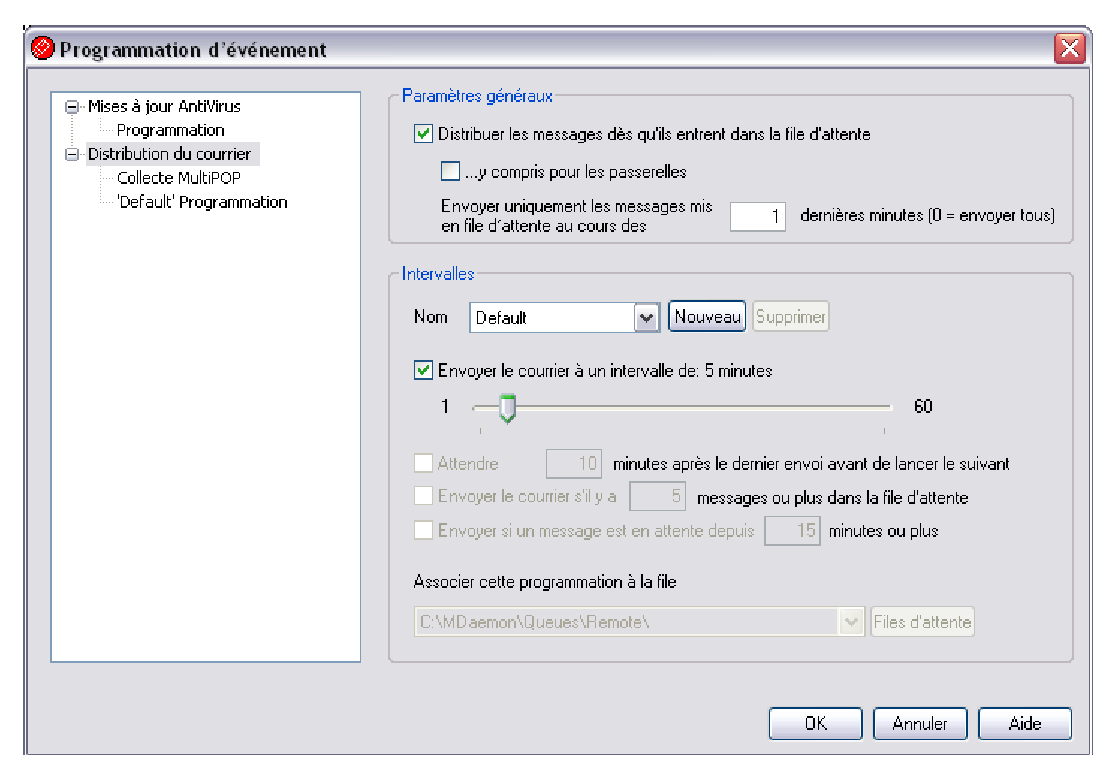
Supprimer les pièces jointes du disque une fois les messages effacés
Sélectionnez cette option si vous souhaitez que les pièces jointes extraites soient supprimées du serveur lorsque le courrier auquel elles sont attachées est effacé. Réfléchissez bien avant d'activer cette option. Si vous le faites et qu'un utilisateur collecte son courrier via un client POP qui n'est pas configuré pour laisser les messages sur le serveur, toutes les pièces jointes qui lui sont destinées seront définitivement perdues. Si cette option n'est pas activée, aucune pièce jointe ne sera perdue, mais une grande partie de votre espace disque pourra être occupée par des fichiers obsolètes et inutiles dont le destinataire d'origine n'a plus besoin ou ne veut plus.

Voir également :

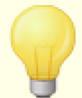
Courrier et pièces jointes 303
Macros de modèles 333
Création de scripts de réponse automatique 343

3.4 Programmation d'événements

3.4.1 Programmation de la distribution du courrier



Pour accéder à cette fenêtre, cliquez sur Configuration » Domaine/Serveurs par défaut » Programmateur d'événements. Cette boîte de dialogue permet de programmer facilement autant de traitements du courrier distant que vous le souhaitez. Vous pouvez programmer la distribution et la collecte de courrier à des heures précises, ou utiliser un compteur pour traiter le courrier à intervalles réguliers. Vous pouvez également définir des conditions qui déclencheront le traitement du courrier à des moments non planifiés, comme par exemple lorsqu'un certain nombre de messages sont en attente de distribution, ou lorsqu'un message est en attente depuis un certain temps. De plus, il est également possible de créer des programmations personnalisées et de les associer à des files d'attente personnalisées. Vous pouvez créer autant de programmations que vous le souhaitez et les utiliser avec n'importe quel type de messages. Par exemple, vous pouvez créer des programmations pour l'envoi de messages volumineux, messages de listes de diffusion, provenant de domaines spécifiques, etc.



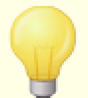
Si vous possédez SecurityPlus for MDaemon 177, vous disposerez d'un onglet supplémentaire dans cette boîte de dialogue qui s'intitule Mises à jour AntiVirus 147. Cet onglet sert à programmer les intervalles de temps au bout desquels les mises à jour des signatures de virus de SecurityPlus sont vérifiées.

Distribution du courrier

Distribuer les messages dès qu'ils entrent dans la file d'attente
Lorsque cette option est activée et qu'un message est reçu dans la file d'attente, MDaemon n'attend pas le prochain cycle de traitement du courrier pour le remettre à son destinataire mais le nombre de minutes indiqué dans l'option ci-dessous.

...y compris pour les passerelles
Cochez cette case si vous souhaitez que l'option précédente s'applique également aux passerelles. Attention, cela ne s'applique qu'aux passerelles pour lesquelles l'option *Distribuer les messages enregistrés à chaque traitement du courrier distant* est cochée (dans l'onglet Domaine 408 des propriétés de la passerelle).

Envoyer uniquement les messages mis en file d'attente au cours des [xx] dernières minutes (0=envoyer tous)
Cette option permet de traiter uniquement les messages mis en file d'attente au cours des XX dernières minutes. Cela augmente l'efficacité du traitement des messages car la réception d'un seul message ne déclenche plus le traitement de tout le courrier. La file continuera d'être traitée entièrement lorsqu'une autre option déclenche cette action. Par défaut, la limite est de 1 minute mais vous pouvez modifier cette valeur ou bien indiquer 0 si nous ne souhaitez pas utiliser cette fonctionnalité (dans ce cas, MDaemon envoie tous les messages en file d'attente chaque fois qu'un message est reçu, ce qui n'est pas efficace).



Les options ci-dessus s'appliquent uniquement à la programmation par défaut (default). Elles ne sont pas disponibles pour les programmations personnalisées.

Nom...
Choisissez dans ce menu déroulant la programmation que vous souhaitez personnaliser. La programmation appelée "Default" est utilisée pour la file distante "traditionnelle" et le courrier DomainPOP et MultiPOP. Si vous utilisez une connexion RAS, la programmation "Default" traitera également la file locale. Cette file contient le courrier de domaines distants pouvant être atteints sans connexion RAS. Les autres programmations peuvent être associées à des files d'attente personnalisées. Pour transférer automatiquement le courrier d'une programmation dans une file personnalisée, utilisez les règles du Filtre de contenu. Après avoir configuré les options de votre choix, cliquez sur OK ou sur Appliquer. Si vous sélectionnez une nouvelle programmation dans le menu déroulant avant d'avoir cliqué sur Appliquer, un message de confirmation s'affiche.

Nouveau
Cliquez sur ce bouton pour créer une nouvelle programmation. Saisissez son nom dans la fenêtre qui s'ouvre ensuite. Une fois la programmation créée, son nom s'affiche dans le menu de gauche. Cliquez sur ce nom pour choisir les heures de traitement du courrier.

Supprimer
Pour supprimer une programmation personnalisée, sélectionnez-la dans le menu déroulant et cliquez sur Supprimer. Un message de confirmation s'affiche alors. Si vous supprimez une programmation personnalisée, la file d'attente et les règles du Filtre de contenu associées seront conservées. Cependant, si vous supprimez une file d'attente personnalisée, les programmations et règles du Filtre de contenu associées le seront également.

Envoyer le courrier à un intervalle de XX minutes
Activez cette option puis déplacez la barre vers la gauche ou la droite pour déterminer l'intervalle de temps entre les différentes sessions de traitement du courrier. Elle peut être placée entre 1 et 60 minutes. Une fois ce temps écoulé, MDaemon traitera le courrier distant avant de recommencer le compte à rebours. Lorsque cette case est décochée, les intervalles de traitement du courrier seront définis par les autres options de programmation dans cette boîte de dialogue.

Attendre XX minutes après le dernier envoi avant de lancer le suivant
Utilisez cette option si vous souhaitez que MDaemon traite à nouveau le courrier un certain nombre de minutes après la fin de chaque session, quel que soit l'événement qui l'ait déclenchée. Contrairement aux options *Envoi programmé* et *Envoyer le courrier à un intervalle de*, le décompte est remis à zéro à chaque traitement du courrier.

Envoyer le courrier s'il y a XX messages ou plus dans la file d'attente
MDaemon déclenche une session de courrier à chaque fois que le nombre de messages de la file distante atteint ou dépasse le nombre que vous avez indiqué ici. Ces sessions s'ajoutent à celles qui sont programmées normalement.

Envoyer le courrier si un message est en attente depuis plus de XX minutes
Lorsque cette option est activée, MDaemon déclenche une session de messagerie à chaque fois qu'un message est en attente dans la file distante depuis le nombre de minutes indiqué. Ces sessions s'ajoutent à celles qui sont programmées normalement.

Files d'attente

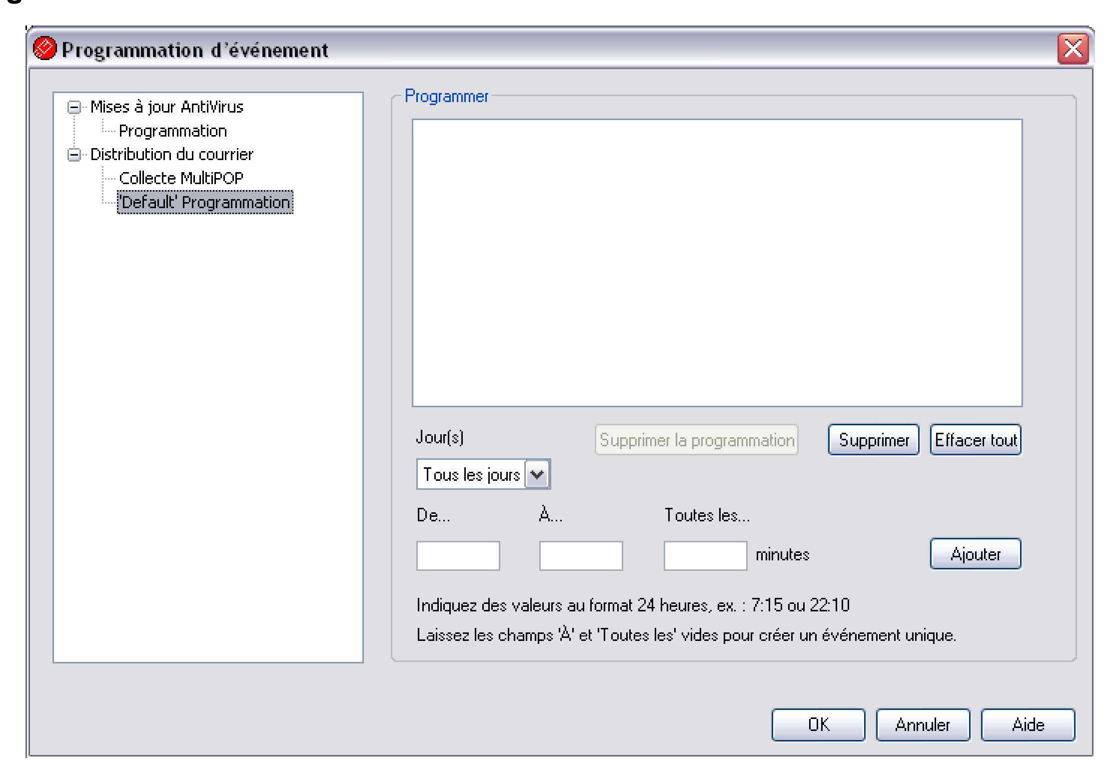
Associer cette programmation à la file
Utilisez cette option pour lier la programmation à une file personnalisée. Il suffit ensuite d'utiliser les règles du Filtre de contenu pour diriger le courrier dans cette file. Par exemple, si vous souhaitez programmer le traitement des messages de liste de diffusion à un horaire spécifique, créez une file personnalisée et une règle destinée à diriger ce type de messages dans cette file.

Files d'attente
Cliquez sur ce bouton pour ouvrir le Gestionnaire de files d'attente 434 et sélectionner une file ou en créer une.

Voir également :

[Programmation de la distribution du courrier](144)
[Mises à jour AntiVirus](147)

3.4.1.1 Programmation



Le nom de chaque programmation correspond à celui figurant dans le menu déroulant *Nom* de l'onglet Distribution du courrier[141]. Les options de cette fenêtre permettent de choisir l'heure à laquelle le courrier de cette programmation va être traité.

Programmer

Supprimer la programmation
Cliquez sur ce bouton pour supprimer la programmation personnalisée (un message de confirmation s'affiche alors). Dans ce cas, elle est également supprimée dans le menu déroulant *Nom* de l'onglet Distribution du courrier[141]. Ce bouton est disponible uniquement pour les programmations personnalisées ; il n'est pas possible de supprimer la programmation Default.

Supprimer
Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Effacer tout
Cliquez sur ce bouton pour supprimer toutes les entrées de la liste.

Envois programmés

Jour(s)
Sélectionnez quels jours vous souhaitez traiter le courrier de cette programmation : tous les jours, jours semaine (du lundi au vendredi), week-end (samedi et dimanche) ou un jour spécifique de la semaine.

De...
Heure à laquelle le traitement du courrier doit commencer (elle doit être au format 24 heures : de 00:00 à 23:59). Si vous souhaitez que le traitement ne soit pas récurrent remplissez uniquement ce champ (et laissez les champs *A...* et *Toutes les...* vides).

A...
Heure à laquelle le traitement du courrier doit s'arrêter pour cette programmation (elle doit être au format 24 heures : de 00:00 à 23:59, et ultérieure à l'heure de début). Laissez ce champ vide si vous souhaitez que cet événement ne soit pas récurrent.

Toutes les [xx] minutes
Intervalle en minutes des traitements du courrier effectués entre les heures indiquées dans les champs *De...* et *A...* Laissez ce champ vide si vous souhaitez que cet événement ne soit pas récurrent.

Ajouter
Après avoir rempli les champs ci-dessus, cliquez sur ce bouton pour ajouter l'entrée à la liste.

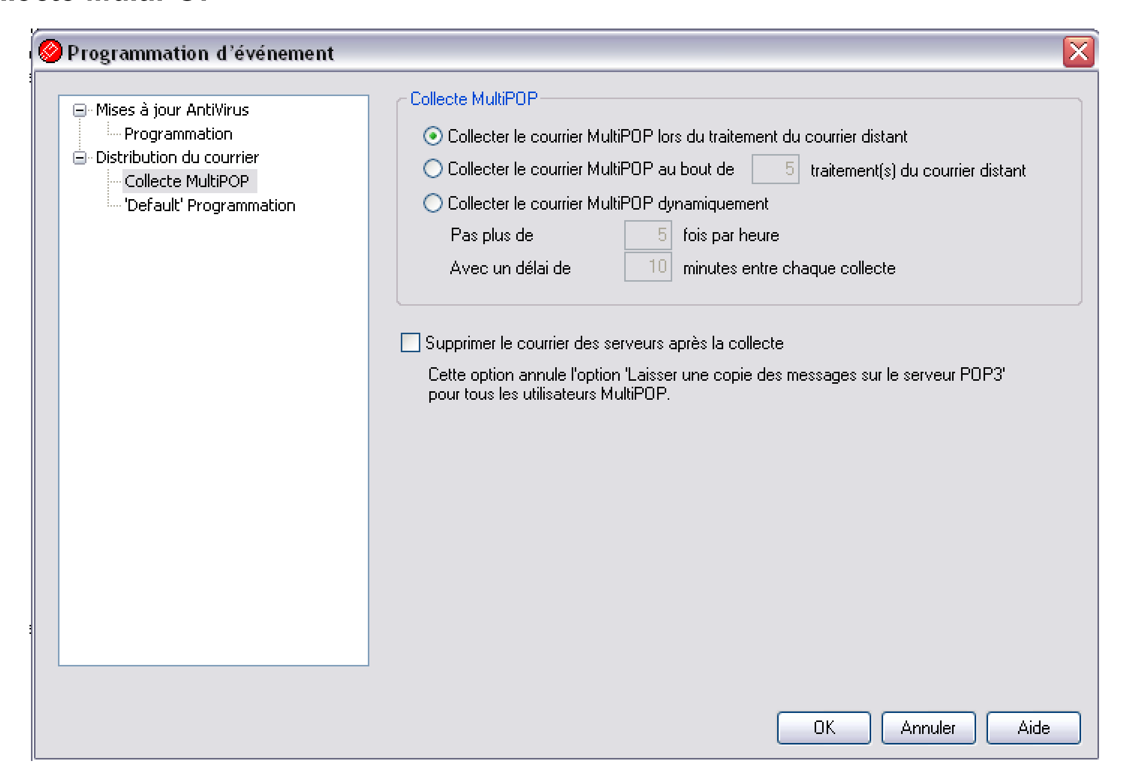


Selon votre configuration, les options de l'onglet Distribution du courrier 141 peuvent suffire à vos besoins. Par exemple, il est inutile de programmer un traitement toutes les minutes chaque jour alors que vous pouvez obtenir le même résultat en plaçant le curseur dans cet onglet à un intervalle d'une minute. Cependant, si vous souhaitez que les intervalles de traitement dépassent 60 minutes chacun, ou qu'ils ne s'appliquent qu'à certains jours, vous pouvez alors utiliser les options de programmation ci-dessus et sélectionner un ou plusieurs jours.

Voir également :

Programmation de la distribution du courrier 141
Mises à jour AntiVirus 147
Mises à jour anti-spam 227

3.4.1.2 Collecte MultiPOP



Collecte MultiPOP

Collecter le courrier MultiPOP lors du traitement du courrier distant
Activez cette option si vous voulez que MDaemon collecte le courrier MultiPOP 320 chaque fois que le courrier distant est traité.

Collecter le courrier MultiPOP au bout de X traitement(s) du courrier distant
Activez cette option et indiquez un nombre dans ce champ si vous voulez que le courrier MultiPOP soit collecté moins souvent que chaque fois que le courrier distant est traité. Ce nombre indique le nombre de fois que sera traité le courrier distant avant que le courrier MultiPOP soit collecté.

Collecter le courrier MultiPOP dynamiquement
Activez cette option si vous voulez collecter le courrier MultiPOP dynamiquement. D'ordinaire, le courrier MultiPOP est collecté pour tous les utilisateurs au même moment à chaque intervalle de traitement du courrier distant ou toutes les x intervalles. Lorsqu'ils sont collectés dynamiquement, les messages MultiPOP le sont pour chaque utilisateur individuel au moment où ils vérifient leur courrier POP, IMAP ou WorldClient plutôt que pour tous les utilisateurs à la fois. Toutefois, comme la collecte MultiPOP est déclenchée par un utilisateur qui vérifie son courrier, tous les nouveaux messages MultiPOP collectés ne seront visibles pour l'utilisateur que lorsqu'il vérifie son courrier à nouveau. Par conséquent, il devra vérifier son courrier à deux reprises afin de voir les nouveaux messages MultiPOP – une première pour déclencher MultiPOP et une seconde pour voir le courrier collecté.

Pas plus de XX fois par heure
Afin de réduire la charge que l'utilisation intensive de MultiPOP peut provoquer dans MDaemon, vous pouvez utiliser cette option pour indiquer le nombre maximum de fois par heure que MultiPOP sera collecté pour chaque utilisateur.

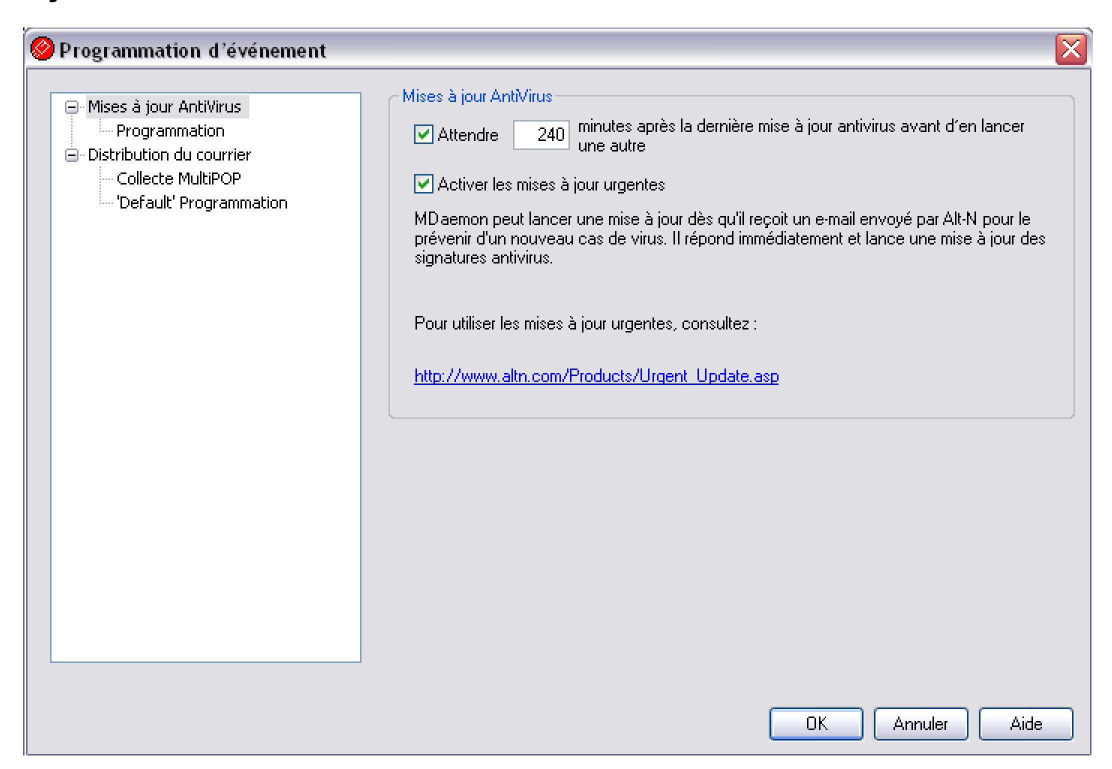
Avec un délai de X minutes entre chaque collecte
Cette option peut permettre de réduire la charge sur le serveur de messagerie en limitant la fréquence de collecte des messages MultiPOP par chaque utilisateur. Elle restreindra la collecte de courrier MultiPOP à un intervalle en minutes par utilisateur. Indiquez le nombre de minutes que vous souhaitez que l'utilisateur doive attendre avant de pouvoir vérifier à nouveau MultiPOP.

Supprimer le courrier des serveurs après la collecte
Cochez cette case si vous souhaiter passer outre l'option Laisser une copie des messages sur le serveur POP (dans l'onglet MultiPOP 320 de l'Éditeur de compte) pour tous les utilisateurs. Tous les messages seront supprimés de chaque serveur MultiPOP après la collecte.

Voir également :

MultiPOP 320

3.4.2 Mises à jour AntiVirus



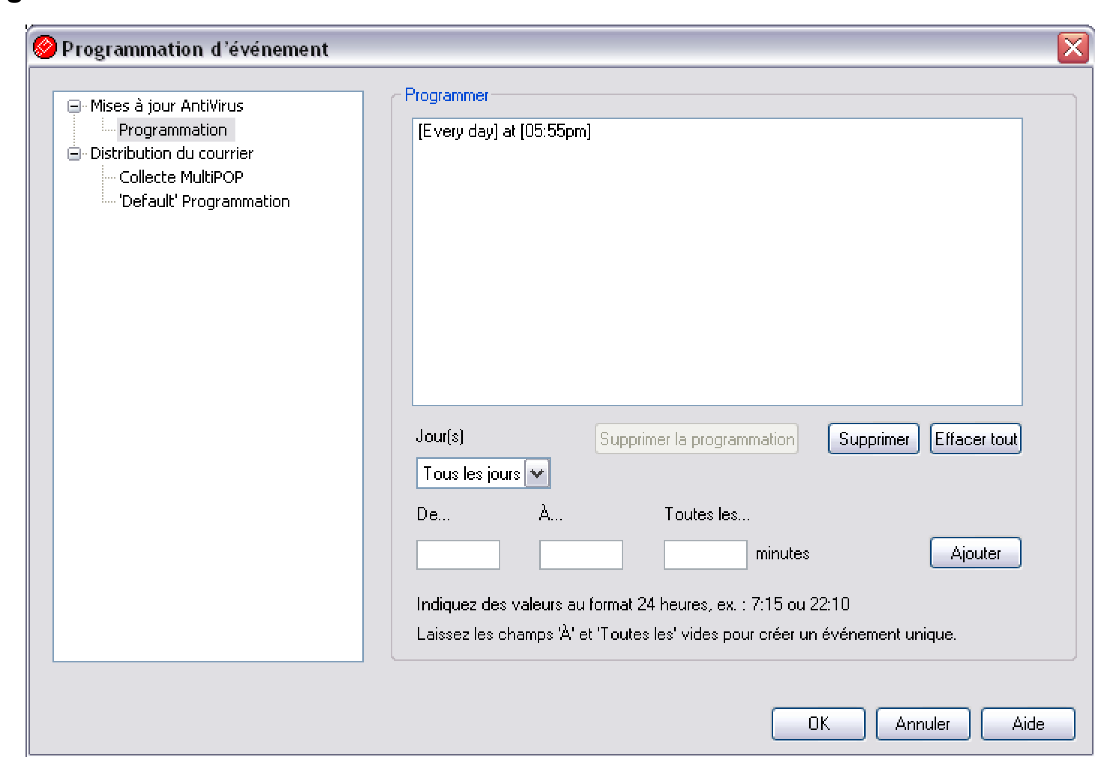
Mises à jour AntiVirus

Attendre X minutes après la dernière mise à jour antivirus avant d'en lancer une autre
Cochez cette case et indiquez le temps (en minutes) que SecurityPlus for MDaemon doit attendre avant la recherche, automatique ou manuelle, des mises à jour des signatures antivirus. Les mises à jour déclenchées par l'une de ces deux méthodes ont la priorité sur cette option. Ainsi, lorsqu'une de ces mises à jour à lieu, le compteur repart à zéro. Par exemple, si cette option est définie pour rechercher les mises à jour toutes les 240 minutes, et que vous vérifiez manuellement une mise à jour 100 minutes plus tard, le compteur repartira alors à 240.

Mises à jour urgentes

Activer les mises à jour urgentes
Cochez cette case pour activer la fonctionnalité Mises à jour urgentes. Lorsqu'elle est activée, SecurityPlus for MDaemon se connecte immédiatement au site où se trouve la mise à jour urgente et la télécharge à chaque fois que MDaemon reçoit le message "Mise à jour urgente". Pour recevoir ces messages, vous devez tout d'abord ajouter votre domaine au système de mises à jour urgentes sur le site altn. com.

3.4.2.1 Programmation



Les options de cette fenêtre permettent de choisir l'heure à laquelle SecurityPlus 177 recherche les nouvelles définitions de virus.

Programmer

Supprimer

Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Effacer tout

Cliquez sur ce bouton pour supprimer toutes les entrées de la liste.

Mises à jour programmées

Jour(s)

Sélectionnez quels jours vous souhaitez rechercher les nouvelles définitions de virus : tous les jours, jours semaine (du lundi au vendredi), week-end (samedi et dimanche) ou un jour spécifique de la semaine.

De...

Heure à laquelle les recherches doivent commencer (elle doit être au format 24 heures : de 00:00 à 23:59). Si vous souhaitez que cet événement ne soit pas récurrent remplissez uniquement ce champ (et laissez les champs *A...* et *Toutes les...* vides).

A...

Heure à laquelle les recherches de nouvelles définitions s'arrêtent (elle doit être au format 24 heures : de 00:00 à 23:59, et ultérieure à l'heure de début). Laissez ce champ vide si vous souhaitez que cet événement ne soit pas récurrent.

Toutes les [xx] minutes

Intervalle en minutes de recherche de nouvelles définitions entre les heures indiquées dans les champs *De...* et *A...*. Laissez ce champ vide si vous souhaitez que cet événement ne soit pas récurrent.

Ajouter

Après avoir rempli les champs ci-dessus, cliquez sur ce bouton pour ajouter l'entrée à la liste.

Voir également :

Mises à jour antivirus 197
Antivirus 197
Utilitaire de mise à jour antivirus 200

3.5 BlackBerry

3.5.1 BlackBerry Internet Service

MDaemon supporte directement le service BlackBerry Internet Service (BIS). Les utilisateurs du service BIS de BlackBerry peuvent à présent intégrer leur compte

MDaemon avec leur BlackBerry et bénéficier du push mail ainsi que d'une meilleure gestion du courrier lors de l'utilisation d'un BlackBerry avec MDaemon. Les BlackBerry configurés pour récupérer leur courrier de MDaemon via IMAP peuvent maintenant être configurés en push mail. De plus, le courrier rédigé sur les BlackBerry est distribué via MDaemon et non via les serveurs BIS. Ainsi, les messages envoyés depuis les BlackBerry sont soumis à la politique de sécurité de votre entreprise : Filtre de contenu, DKIM, archivage, etc.

BIS collecte uniquement le courrier se trouvant dans la boîte de réception, ce qui peut être génant pour les utilisateurs ayant créé des filtres IMAP 307 pour classer automatiquement les messages dans des dossiers spécifiques. Afin d'éviter ce problème, l'onglet Courrier BlackBerry 325 de l'Éditeur de compte et la page Dossiers de WorldClient permettent respectivement aux administrateurs et aux utilisateurs de choisir les dossiers à synchroniser. Lorsque le service BIS se connecte à MDaemon pour collecter le courrier, MDaemon envoie le contenu des dossiers sélectionnés. Tous les messages provenant des dossiers sélectionnés sont envoyés dans le dossier Messages du BlackBerry. Ces messages restent dans leurs dossiers respectifs sur le serveur MDaemon et les dossiers ne sont pas créés sur le BlackBerry. Ils sont simplement envoyés sur le BlackBerry comme s'ils appartenaient au dossier de courrier.

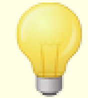
Enfin, un système d'alias interne lie les dossiers Éléments envoyés et Éléments supprimés (quels que soient leurs noms) à des valeurs reconnues par BIS. Cela permet de s'assurer que les messages envoyés et supprimés soient placés dans les dossiers correspondants de MDaemon.

La boîte de dialogue BlackBerry Internet Service contient les onglets suivants :

Domaines 151 — permet d'activer l'intégration avec BIS pour les domaines souhaités. Cet onglet affiche un historique des souscriptions, et contient diverses options SSL et STARTTLS.

Comptes intégrés 153 — affiche la liste des comptes configurés pour le push mail avec BIS et donc directement intégrés dans MDaemon. Même si un compte ne figure pas dans cette liste, un serveur BIS pourra collecter le courrier pour le BlackBerry via POP3 ou IMAP, mais ce compte ne pourra pas envoyer son courrier via votre serveur MDaemon.

Options 155 — contient divers options globales d'intégration de MDaemon avec BlackBerry. Par exemple, vous pouvez autoriser la synchronisation de dossiers autres que "Courrier", choisir d'appliquer les liens vers les pièces jointes 139, autoriser l'intégration de plusieurs BlackBerry avec un seul compte MDaemon, ainsi que diverses options.



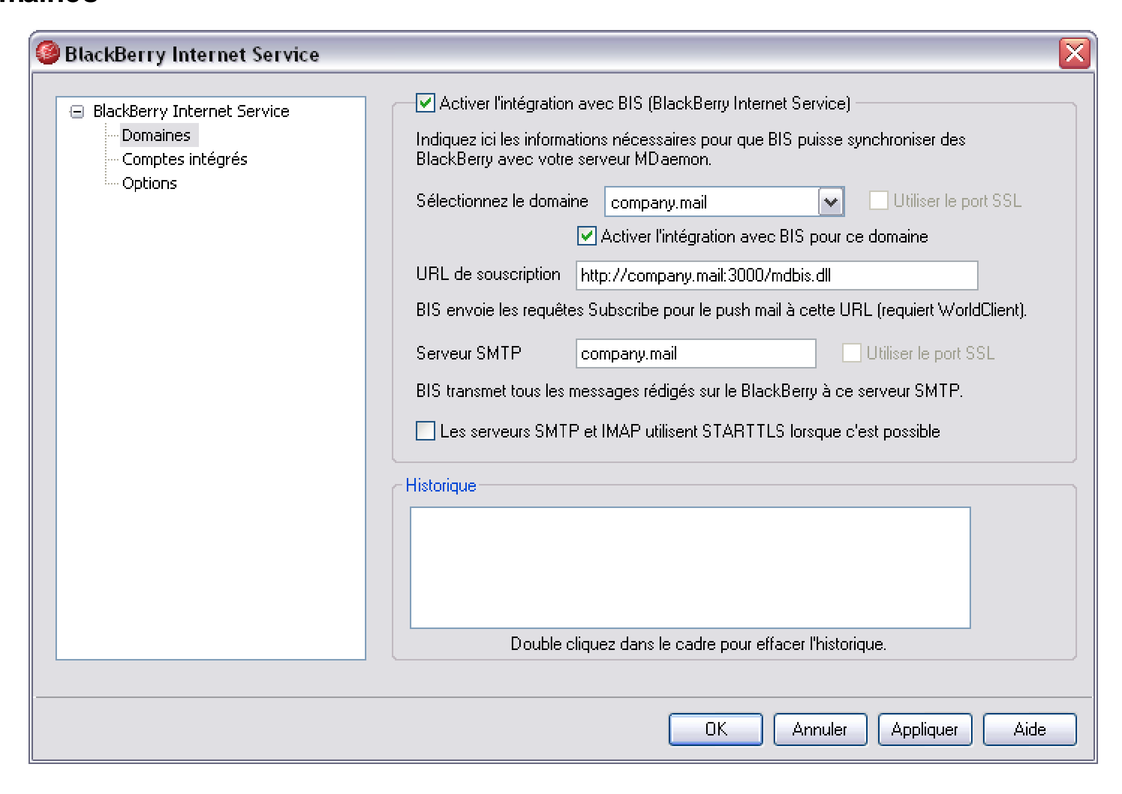
MDaemon requiert que toutes les sessions IMAP/POP d'utilisateurs de BlackBerry utilisent leur adresse e-mail complète en tant que nom d'utilisateur pour la collecte IMAP et/ou POP. Ainsi, lors de la création du profil de messagerie sur le BlackBerry, les utilisateurs devront indiquer l'adresse e-mail complète pour le nom d'utilisateur. Cela est nécessaire pour éviter d'éventuels conflits et intégrer correctement les comptes. Certains utilisateurs ayant déjà créé un profil de messagerie devront le supprimer et le recréer ou modifier leur

nom d'utilisateur.

Voir également :

[BlackBerry » Domaines] 151
[Comptes intégrés] 153
[BlackBerry » Options] 155
[Courrier BlackBerry] 325

3.5.1.1 Domaines



Activer l'intégration avec BIS (BlackBerry Internet Service)
Cochez cette case si vous souhaitez activer l'intégration de MDaemon avec BIS pour le domaine sélectionné.



Lorsque l'intégration BIS est désactivée de façon globale ou pour un domaine spécifique, tous les comptes déjà configurés continueront de fonctionner comme avant. Seule l'intégration de nouveaux comptes est désactivée, les comptes existants ne sont pas concernés par cette option.

Sélectionnez le domaine
Sélectionnez dans ce menu déroulant le domaine pour lequel vous souhaitez configurer l'intégration avec BIS. Toutes les modifications apportées aux autres

options de cet onglet s'appliquent uniquement à ce domaine.

Activer l'intégration avec BIS pour ce domaine
Cochez cette case pour activer l'intégration avec BIS pour le domaine sélectionné.

Utiliser le port SSL
Si vous avez activé SSL272 dans MDaemon, cochez cette case pour que le client IMAP de BIS utilise le port SSL dédié. Le client IMA de BIS supporte uniquement le port SSL dédié.

URL de souscription
URL de WorldClient à laquelle le serveur BIS envoie les requêtes subscribe et unsubscribe. Lorsqu'un utilisateur configure le compte de messagerie sur son BlackBerry, BIS envoie une requête de souscription à cette URL dans les 20 minutes qui suivent environ. MDaemon ajoute alors le compte à la liste des Comptes intégrés153. Les requêtes étant traitées par WorldClient, ce dernier doit bien sûr être actif.

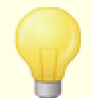
Serveur SMTP
Serveur SMTP auquel sont envoyés les messages rédigés sur le BlackBerry pour être distribués.

Utiliser le port SSL
Si vous avez activé SSL272 dans MDaemon, cochez cette case pour que le client SMTP de BIS utilise le port SSL dédié.



Le client SMTP de BIS ne supporte pas actuellement SSL avec des certificats autosignés. Par conséquent, si vous souhaitez utiliser SSL vous devez utiliser un certificat tiers commercial.

Les serveurs SMTP et IMAP utilisent STARTTLS lorsque c'est possible
Si vous avez activé STARTTLS272 dans MDaemon, cochez cette case pour que les serveurs SMTP et IMAP utilisent STARTTLS lorsque c'est possible.



BIS ne supporte pas STARTTLS avec des certificats autosignés. Par conséquent, si vous souhaitez utiliser STARTTLS vous devez utiliser un certificat tiers commercial.

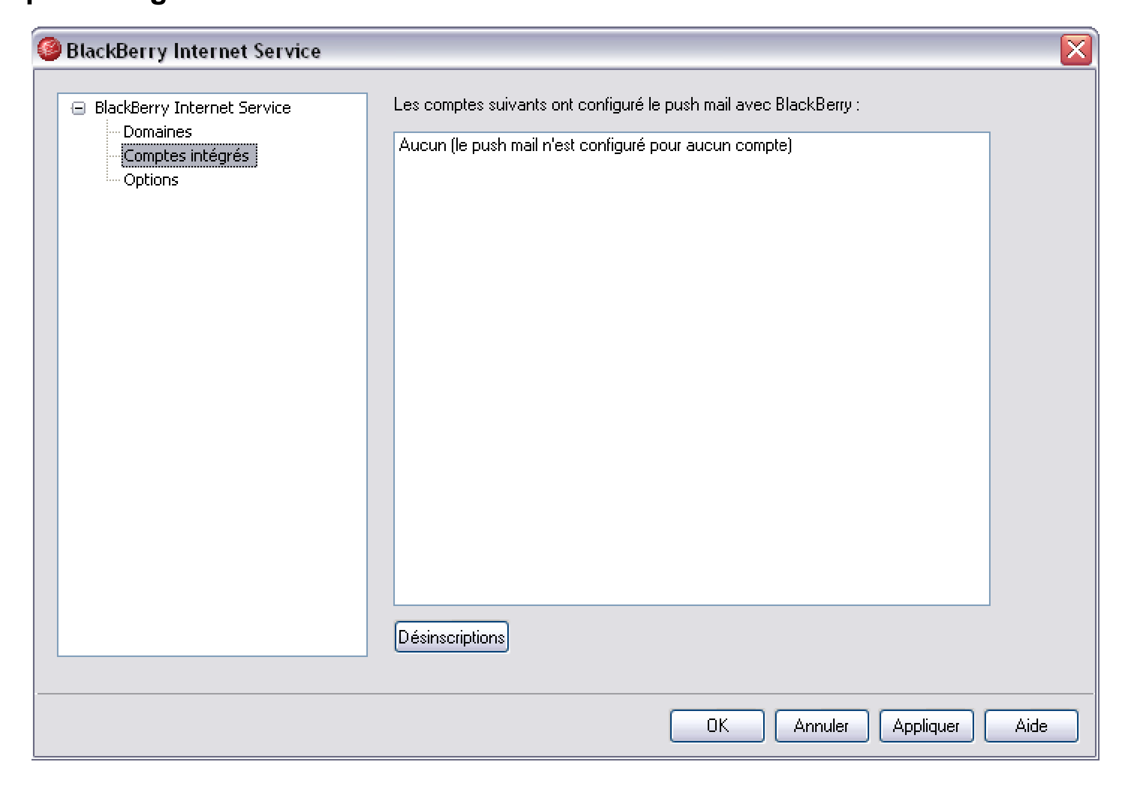
Historique

Historique BIS pour vos comptes. Chaque entrée indique s'il s'agit d'une requête subscribe ou unsubscribe, l'adresse e-mail ainsi que la date et l'heure.

Voir également :

[BlackBerry Internet Service](149)
[Comptes intégrés](153)
[BlackBerry » Options](155)
[Courrier BlackBerry](325)

3.5.1.2 Comptes intégrés



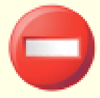
Comment configurer un compte MDaemon pour le push mail avec BlackBerry

Cet onglet affiche la liste des comptes intégrés. Pour configurer un nouveau compte :

1. Activez les options d'intégration avec BIS pour le serveur et le domaine dans l'onglet Domaines 151, et assurez-vous que l'URL de souscription pointe vers votre serveur WorldClient et que la valeur Serveur SMTP pointe vers votre serveur SMTP MDaemon.
2. Si le BlackBerry collecte déjà du courrier sur le compte MDaemon, cela signifie qu'un profil a déjà été créé sur le BlackBerry pour le compte MDaemon. Ce profil doit être supprimé (il est nécessaire de recréer le profil pour déclencher le push mail dans BIS).
3. Configurez le compte MDaemon sur le BlackBerry de l'utilisateur, en indiquant

l'adresse e-mail complète en tant que nom d'utilisateur. Pour savoir comment créer un profil de messagerie sur un BlackBerry, consultez l'aide en ligne ou la documentation du BlackBerry. Une fois le compte ajouté, vous ne devez pas modifier la signature ou les options avancées. Vous pourrez effectuer les modifications souhaitées à l'étape 6.

4. Une fois le profil créé, l'URL de souscription associée au domaine auquel l'utilisateur appartient reçoit une requête SUBSCRIBE du service BIS. Cette requête est traitée automatiquement par WorldClient et le compte est ajouté à la liste des comptes intégrés. La requête SUBSCRIBE met environ 5 minutes à arriver, mais cela peut prendre jusqu'à 20 minutes.
5. Presque aussitôt après la création l'utilisateur reçoit un message d'information sur l'activation. Puis, une fois la requête SUBSCRIBE traitée, le BlackBerry reçoit un deuxième message d'information sur l'activation du push mail. Une fois le deuxième message reçu, cela signifie que le push mail est correctement configuré pour ce compte.
6. Vous pouvez alors effectuer les modifications souhaitées sur le profil (signatures, options avancées, etc.).



Tant que la requête SUBSCRIBE de BIS n'a pas été reçue et traitée, toute modification apportée aux paramètres du profil empêchera sa réception (signature, options avancées, etc.). Par conséquent, une fois le profil créé, vous ne devez pas y apporter de modifications jusqu'à la réception du message de confirmation. Sinon, vous devrez supprimer le compte et le recréer pour relancer la procédure de souscription.



Un tel niveau d'intégration n'est pas possible en POP. Si des utilisateurs de BlackBerry collectent leur courrier en POP, ils devront supprimer leur profil et en recréer un nouveau utilisant IMAP. Le serveur IMAP de MDaemon doit bien sûr être démarré pour que cet outil fonctionne.

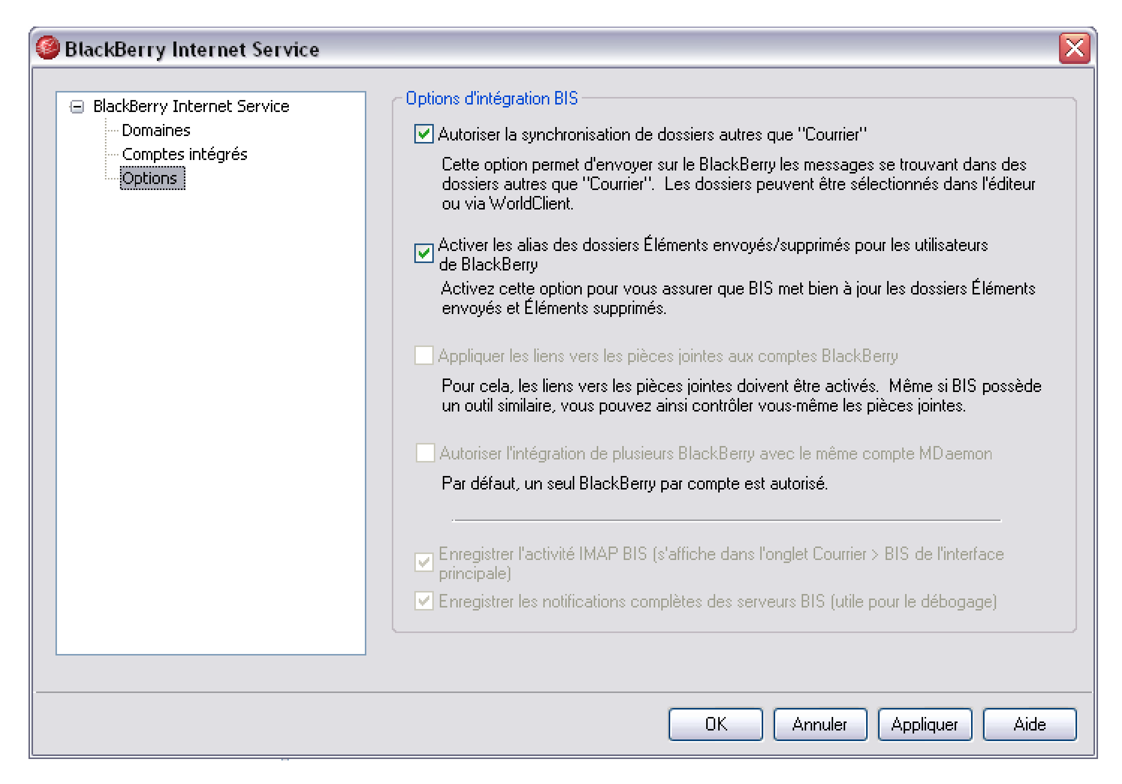
Désinscription d'un compte intégré

Pour "désinscrire" le compte du push mail, il suffit de supprimer le profil sur le BlackBerry. BIS envoie alors à MDaemon une requête UNSUBSCRIBE. Le traitement de la requête UNSUBSCRIBE peut être un peu long mais cela ne perturbe pas le fonctionnement de l'appareil.

Voir également :

BlackBerry Internet Service 149
BlackBerry » Domaines 151
BlackBerry » Options 155
Courrier BlackBerry 325

3.5.1.3 Options



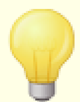
Options d'intégration BIS

Autoriser la sélection de dossiers autres que "Courrier"
Les messages se trouvant dans des dossiers IMAP autres que le dossier Courrier racine peuvent être envoyés sur le BlackBerry. Ils peuvent être sélectionnés dans l'onglet Courrier BlackBerry 325 de l'Éditeur de compte pour l'administrateur et la page Dossiers de WorldClient pour l'utilisateur. Si vous ne souhaitez pas autoriser les utilisateurs à sélectionner d'autres dossiers, décochez cette option. Il est cependant recommandé de laisser cette option activée, car sinon les utilisateurs ayant créé des Filtres IMAP 307 pour classer automatiquement les messages dans des dossiers spécifiques ne recevront pas les messages de ces dossiers sur leur BlackBerry.



Cette fonctionnalité est indépendante des options d'intégration des onglets Domaines 151 et Comptes intégrés 153. Même si vous désactivez l'intégration avec BIS dans MDaemon, l'utilisateur peut tout de même créer un profil de messagerie sur son BlackBerry pour collecter son courrier de MDaemon ; tout comme avec n'importe quel client de messagerie traditionnel ou smartphone. Cette option permet simplement de collecter le courrier dans d'autres dossiers en plus du dossier Courrier racine.

Activer les alias des dossiers Élements envoyés/supprimés pour les utilisateurs de BlackBerry
Un système d'alias interne lie les dossiers Éléments envoyés et Éléments supprimés (quels que soient leurs noms) à des valeurs reconnues par BIS. Les noms des dossiers ne sont pas altérés, ce système est entièrement interne et permet de s'assurer que les messages envoyés et supprimés soient placés dans les dossiers correspondants de MDaemon. Tout comme l'option ci-dessus, cette option est indépendante des paramètres d'intégration. Elle peut être utilisée même si l'option *Activer l'intégration avec BIS* est désactivée dans l'onglet Domaines.



Les utilisateurs peuvent sélectionner les dossiers Élements envoyés/supprimés de leur choix dans la page Dossiers de WorldClient.

Appliquer les liens vers les pièces jointes aux comptes BlackBerry
Cochez cette case si vous souhaitez appliquer le sysème de Liens vers les pièces jointes 139 aux messages envoyés aux comptes intégrés 153 avec BlackBerry. Les liens vers les pièces jointes doivent être activés pour que cette option fonctionne.

Autoriser l'intégration de plusieurs BlackBerry avec le même compte MDaemon
Activez cette option si vous souhaitez autoriser l'intégration du plusieurs BlackBerry pour un même compte MDaemon. Ainsi, si un utilisateur possède deux smartphones BlackBerry il peut recevoir le courrier de son compte MDaemon sur les deux appareils.

Enregistrer l'activité IMAP BIS (s'affiche dans l'onglet Courrier > BIS de l'interface principale)
Cochez cette case si vous souhaitez enregistrer l'activité IMAP de BIS. Les données seront affichées dans l'onglet Courrier > BIS de l'interface principale et enregistrées dans les fichiers journaux.

Enregistrer les notifications complètes des serveurs BIS (utile pour le déboggage)
Cochez cette case si vous souhaitez enregistrer dans les fichiers journaux toute l'activité des serveurs BIS. Cette option peut être utile pour diagnostiquer d'éventuels problèmes liés à BIS.

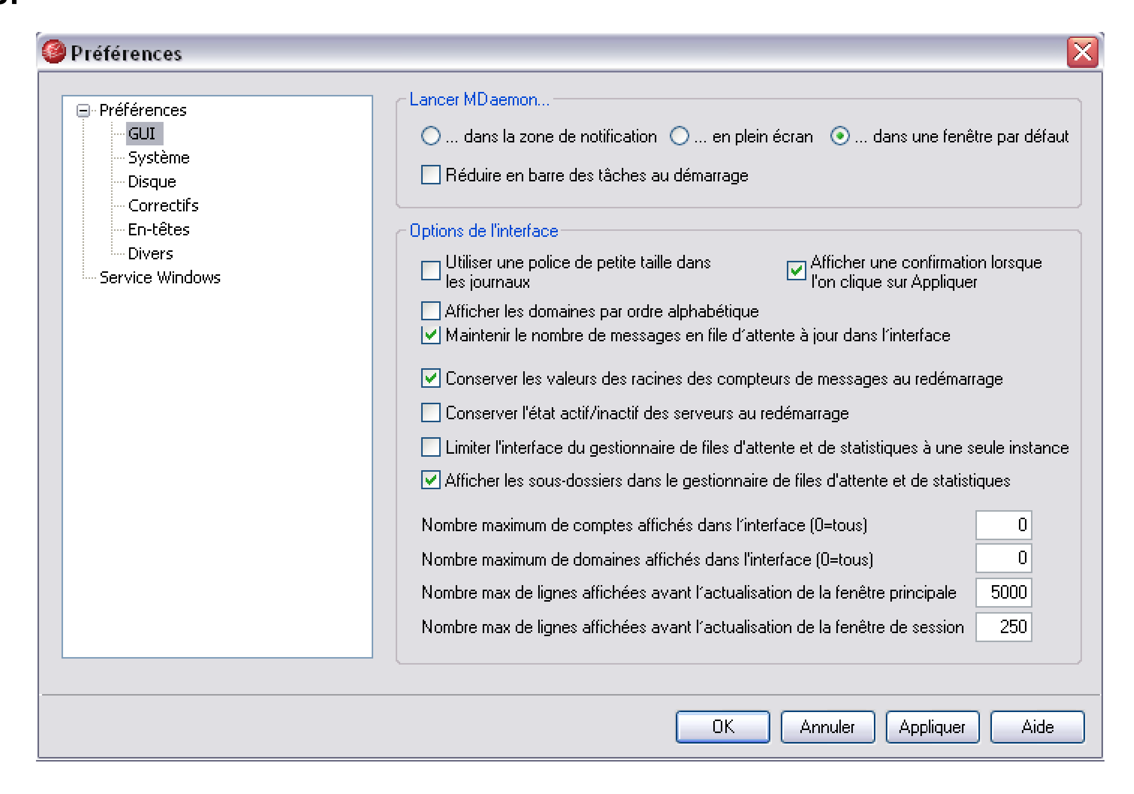
Voir également :

BlackBerry Internet Service 149
BlackBerry » Domaines 151
Comptes intégrés 153
Courrier BlackBerry 325

3.6 Préférences

3.6.1 Préférences

3.6.1.1 GUI



Lancer MDaemon...

...dans la zone de notification
Choisissez cette option si vous voulez que l'interface de MDaemon soit réduite au démarrage. Seule l'icône de la zone de notification s'affiche.

...en plein écran
Choisissez cette option si vous voulez que l'interface de MDaemon s'affiche dans une fenêtre en plein écran au démarrage.

...dans une fenêtre par défaut
Choisissez cette option si vous voulez que l'interface de MDaemon s'affiche dans une fenêtre par défaut au démarrage.

Réduire en barre des tâches au démarrage
Lorsque cette option est activée MDaemon est réduit en barre des tâches au démarrage (l'icône de la zone de notification s'affiche également).

Options de l'interface

Utiliser une police de petite taille dans les journaux
Affiche une police de petite taille dans les onglets de l'interface principale.

Afficher une confirmation lorsque l'on clique sur Appliquer
Par défaut, lorsque l'on clique sur le bouton Appliquer un message de confirmation s'affiche indiquant que les modifications ont bien été enregistrées. Décochez cette case si vous ne souhaitez pas afficher ce message de confirmation.

Afficher les domaines par ordre alphabétique
Sélectionnez cette option pour que la liste des domaines soit triée par ordre alphabétique dans les options de MDaemon. Si cette option est désactivée, les domaines seront répertoriés dans leur ordre d'apparition dans le fichier domains.dat situé dans le répertoire \app\ de MDaemon. Lorsque vous modifiez ce paramètre, le nouvel ordre de tri apparaîtra dans l'interface utilisateur après avoir redémarré le MDaemon.

Maintenir le nombre de messages en file d'attente à jour dans l'interface
Lorsque cette option est activée, MDaemon vérifie le nombre de messages en file d'attente sur le disque.

Conserver les valeurs des racines des compteurs de messages au redémarrage
Activez cette option si vous souhaitez que les valeurs des racines de l'arborescence de l'onglet Statistiques ne soient pas remises à zéro à chaque redémarrage de MDaemon.

Conserver l'état actif/inactif du serveur au redémarrage
Si cette option est activée, MDaemon s'assure que l'état de ses serveurs (active ou désactivé) reste le même après un redémarrage.

Limiter l'interface du gestionnaire de files d'attente et de statistiques à une seule instance
Activez cette option si vous souhaitez empêcher l'exécution simultanée de plusieurs instances du gestionnaire de files d'attente et de statistiques 437.

Afficher les sous-dossiers dans le gestionnaire de files d'attente et de statistiques
Activez cette option si vous voulez que le gestionnaire de statistiques de files d'attente affiche les sous-dossiers contenus dans les différentes files d'attente et les dossiers de messagerie des utilisateurs.

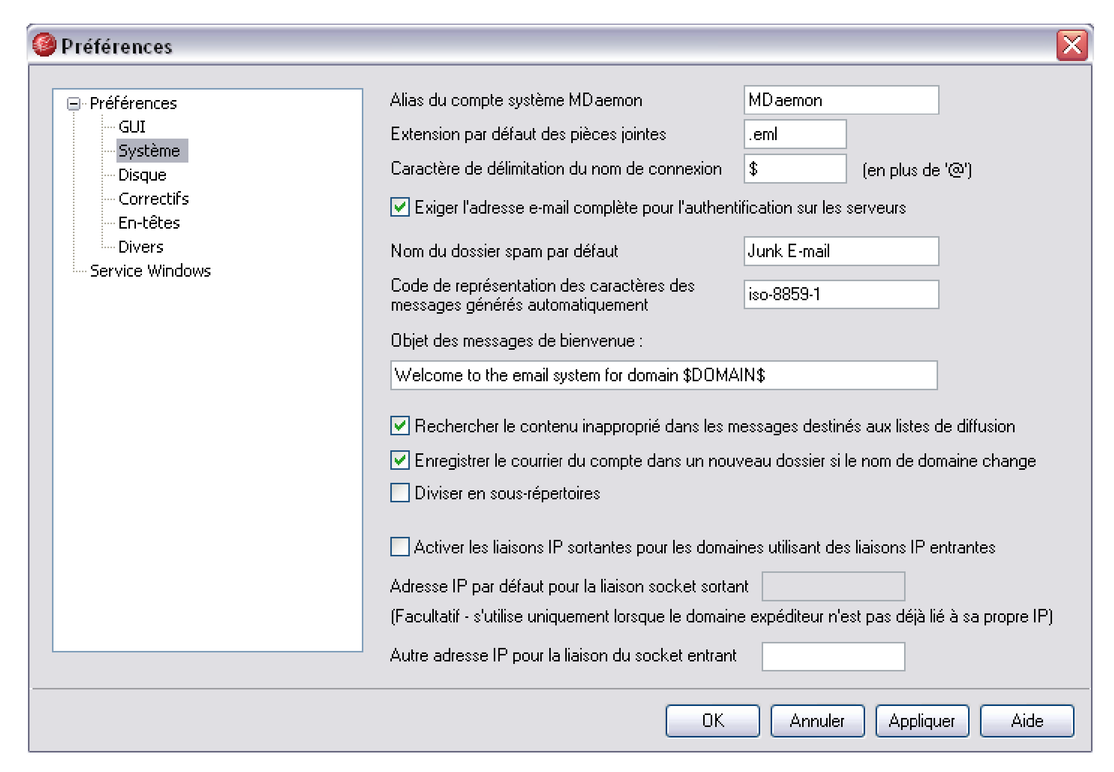
Nombre max. de comptes affichés dans l'interface (0=tous)
Il s'agit du nombre maximum de comptes qui seront affichés dans les listes de choix des différentes boîtes de dialogue. De plus, lorsque la valeur de cette commande est définie sur autre chose que "0" (afficher tout) les options *Modifier un compte* et *Supprimer un compte* n'apparaîtront plus dans le menu Comptes. Ces fonctions ne seront disponibles que depuis le gestionnaire de comptes. Vous devez redémarrer MDaemon pour que les modifications apportées à cette option soient appliquées. Par défaut, tous les comptes sont affichés.

Nombre max. de domaines affichés dans l'interface (0=tous)
Nombre maximum de domaines supplémentaires affichés dans l'interface principale. Vous devez redémarrer MDaemon pour que les modifications apportées à cette option soient appliquées. Il n'est pas possible d'indiquer une valeur inférieure à 50. Par défaut, tous les domaines sont affichés.

Nombre max de lignes affichées avant l'actualisation de la fenêtre principale
Il s'agit du nombre maximum de lignes qui seront affichées dans la fenêtre principale de MDaemon. Lorsque ce nombre de lignes est atteint, la fenêtre sera actualisée. Cela n'a pas d'incidence sur le fichier journal. Seul l'affichage est actualisé.

Nombre max de lignes affichées avant l'actualisation de la fenêtre de session
Il s'agit du nombre maximum de lignes qui s'afficheront dans chaque onglet Session 27 avant que leur contenu ne soit actualisé. Cela n'a pas d'incidence sur les fichiers journaux.

3.6.1.2 Système



Alias du compte système MDaemon
Il s'agit de l'adresse électronique d'où proviendront les messages générés par le système (confirmations d'abonnement, messages "Impossible de distribuer", divers messages de notification, etc.).

Extension par défaut des pièces jointes
Les messages générés par le système seront créés à l'aide de cette extension. Cette extension est également attribuée aux pièces jointes incluses dans les messages générés par le système. Par exemple, si MDaemon génère un message d'avertissement au postmaster concernant un message particulier, il mettra ce message en pièce jointe avec l'extension indiquée.

Caractère de délimitation du nom de connexion (chaîne de 10 caractères max)
Lorsque vous utilisez une adresse électronique comme paramètre de connexion de compte, ce caractère ou cette chaîne de caractères peuvent être utilisés comme alternative à "@". Cela peut être nécessaire à certains utilisateurs dont les clients de messagerie ne prennent pas en charge le caractère "@" dans le champ de connexion. Par exemple, si vous utilisez "$" dans ce champ, les utilisateurs peuvent alors se connecter à l'aide de "utilisateur@domaine.com" ou "utilisateur$domaine.com".

Exiger l'adresse e-mail complète pour l'authentification sur les serveurs
Les serveurs POP et IMAP de MDaemon exigent l'adresse e-mail complète pour l'authentification. Décochez cette case si vous souhaitez autoriser l'authentification avec uniquement le nom de la boîte aux lettres (ex. : "frank" au lieu de "frank@exemple.com"). Cependant, ceci est fortement déconseillé car les connexions utilisant uniquement le nom de la boîte sont ambigües lorsque MDaemon contient plusieurs domaines.

Nom du dossier spam par défaut
Précise le nom du dossier spam par défaut que MDaemon créera automatiquement pour vos utilisateurs. Pour correspondre avec les paramètres par défaut de nombreux autres logiciels, le nom par défaut est "Junk E-mail".

Code de représentation des caractères des messages générés automatiquement
Indiquez le jeu de caractères que vous souhaitez utiliser pour les messages générés automatiquement. Le paramètre par défaut est iso-8859-1.

IP secondaire pour une liaison en double socket
Si vous voulez que le domaine par défaut soit lié à une adresse IP supplémentaire, incluez-la ici.

Objet des messages de bienvenue
MDaemon envoie un message de bienvenue aux nouveaux comptes. Indiquez ici l'objet de ce message (en-tête "Subject"). Le message de bienvenue est créé à partir du fichier `NEWUSERHELP.DAT` situé dans le répertoire …/MDaemon/app/. L'en-tête "Subject" peut contenir toutes les macros autorisées dans les scripts de réponse automatique 343.

Rechercher le contenu inapproprié dans les messages destinés aux listes de diffusion
Lorsqu'un message arrive pour une liste de diffusion et aurait du être dirigé vers l'adresse système, MDaemon le rejette si cette commande est activée. Par exemple, un utilisateur peut s'inscrire ou quitter une liste en mettant la commande Subscribe ou Unsubscribe en début d'un message et l'envoyer à l'adresse système. Souvent, les utilisateurs essayent d'envoyer par erreur ces messages à la liste elle-tmême. En activant cette commande, ces messages ne pourront pas être envoyés à la liste.

Enregistrer le courrier du compte dans un nouveau dossier si le nom de domaine change
Si cette option est activée lorsque vous renommez un domaine, le courrier du compte de ce domaine sera déplacé vers les dossiers portant un nouveau nom. Sinon, MDaemon continuera d'utiliser les noms des anciens dossiers de messagerie.

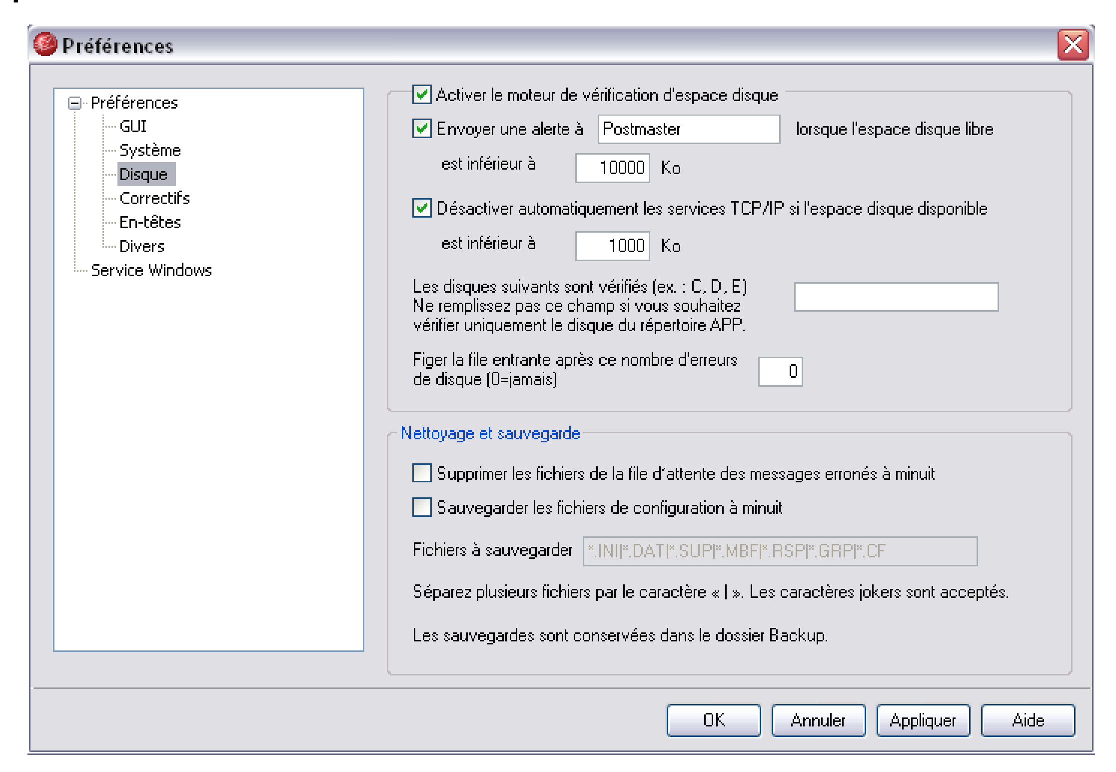
Diviser en sous-répertoires
Activez cette option si vous souhaitez activer la division des répertoires - MDaemon divise certains répertoires en 65 sous-répertoires. Cette division permet d'augmenter les performances de certains sites volumineux mais peut réduire légèrement les performances des installations "traditionnelles". Cette option est désactivée par défaut.

Activer les liaisons IP sortantes pour les domaines utilisant des liaisons IP entrantes
Cochez cette option pour que les domaines utilisant l'option *Lier les sockets d'écoute à cette IP* effectuent aussi des liaisons sur les sockets sortants. L'adresse IP utilisée est la même que celle utilisée pour le traitement du courrier entrant, sauf si une adresse spécifique est indiquée ci-dessous :

Adresse IP par défaut pour la liaison socket sortant
Adresse IP utilisée pour la liaison du socket sortant. Cette option est facultative et uniquement nécessaire si le domaine n'est pas déjà lié à sa propre IP.

Autre adresse IP pour la liaison du socket entrant
Si vous voulez que le domaine par défaut soit lié à une adresse IP supplémentaire, incluez-la ici.

3.6.1.3 Disque



Activer le moteur de vérification d'espace disque
Activez cette option si vous voulez que MDaemon vérifie l'espace disque disponible

sur le lecteur où MDAEMON.EXE est situé.

Envoyer une alerte à [utilisateur ou adresse] lorsque l'espace disque libre est inférieur à XX Ko
En utilisant cette option, vous pouvez configurer MDaemon pour qu'il envoie un message de notification à l'utilisateur ou à l'adresse de votre choix dès que l'espace disque est inférieur à un certain seuil.

Désactiver les services TCP/IP si l'espace disque disponible est inférieur à XX Ko
Activez cette fonctionnalité si vous voulez que MDaemon désactive les services TCP/IP dès que l'espace disque est inférieur à un certain seuil.

Les disques suivants sont vérifiés (ex : C, D, E)
Si vous souhaitez surveiller l'espace disque sur plusieurs lecteurs, indiquez ici les lettres des lecteurs à surveiller. Si vous ne remplissez pas ce champ, seul le lecteur contenant le répertoire `\app\` de MDaemon sera vérifié.

Figer la file entrante après ce nombre d'erreurs de disque (0=jamais)
Si le nombre d'erreurs indiqué se produit lors du traitement de la file entrante, MDaemon arrête le traitement de cette file jusqu'à ce que le problème soit résolu. Dans ce cas, un message d'avertissement est placé dans la boîte du postmaster.

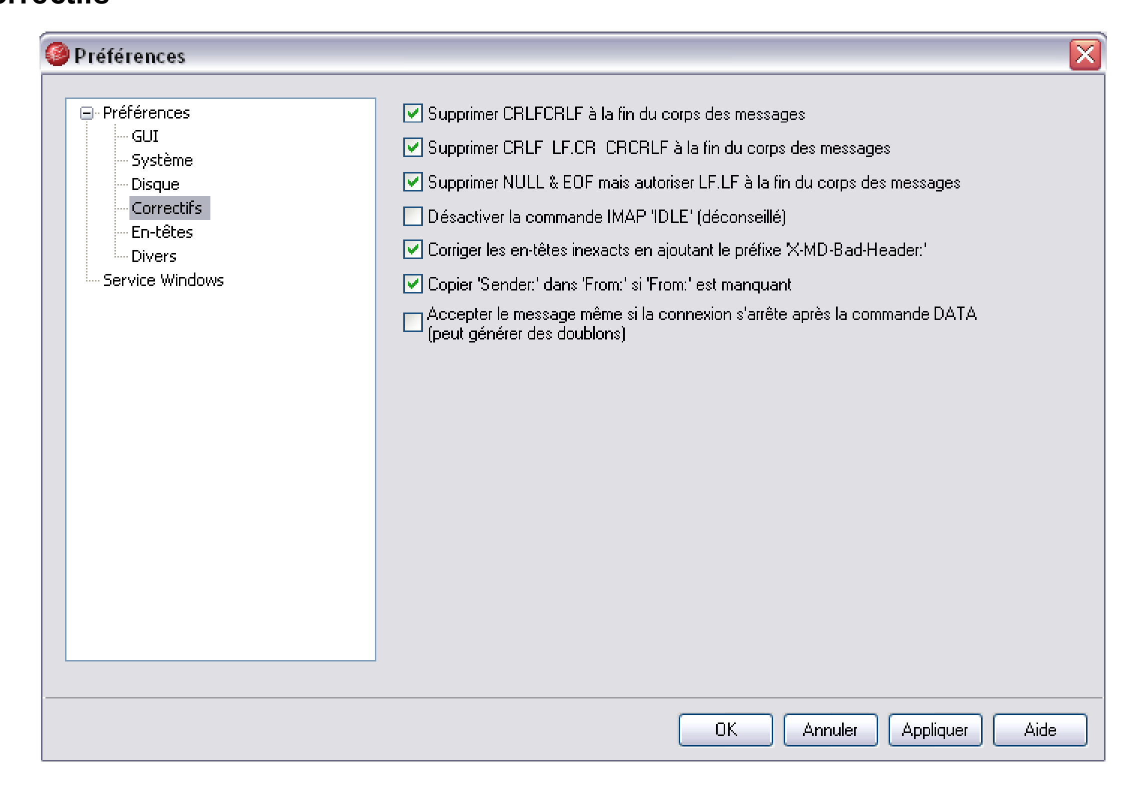
Nettoyage et sauvegarde

Supprimer les fichiers de la file d'attente des messages erronés à minuit
Activez cette option si vous voulez que MDaemon supprime tous les fichiers de la file d'attente des messages erronés chaque nuit à minuit. Cela permet d'économiser de l'espace disque.

Sauvegarder les fichiers de configuration à minuit
Activez cette option si vous voulez archiver tous les fichiers de configuration MDaemon chaque soir à minuit dans le répertoire "Backups".

Fichiers à sauvegarder
Utilisez cette zone de texte pour indiquer exactement les fichiers et les extensions de fichier à sauvegarder. Les jokers sont autorisés et chaque nom de fichier ou extension doit être séparé par le caractère "|".

3.6.1.4 Correctifs



Supprimer CRLFCRLF à la fin du corps des messages
Certains clients de messagerie rencontrent des problèmes pour afficher messages terminant par plusieurs retours à la ligne consécutifs (CRLFCRLF). Lorsque cette option est activée, MDaemon retire les séquences CRLFCRLF consécutives à la fin du corps du message.

Supprimer CRLF LF.CR CRCRLF à la fin du corps des messages
Par défaut, MDaemon supprime cette séquence lorsqu'elle se trouve à la fin des messages car cela peut causer des problèmes avec certains clients de messagerie.

Supprimer NULL & EOF mais autoriser LF.LF à la fin du corps des messages
Lorsque cette option est activée, MDaemon supprime `Null` et EOF à la fin du corps des messages, mais conserve `LF.LF` et la séquence `CRLF.CRLF` indiquant la fin du message.

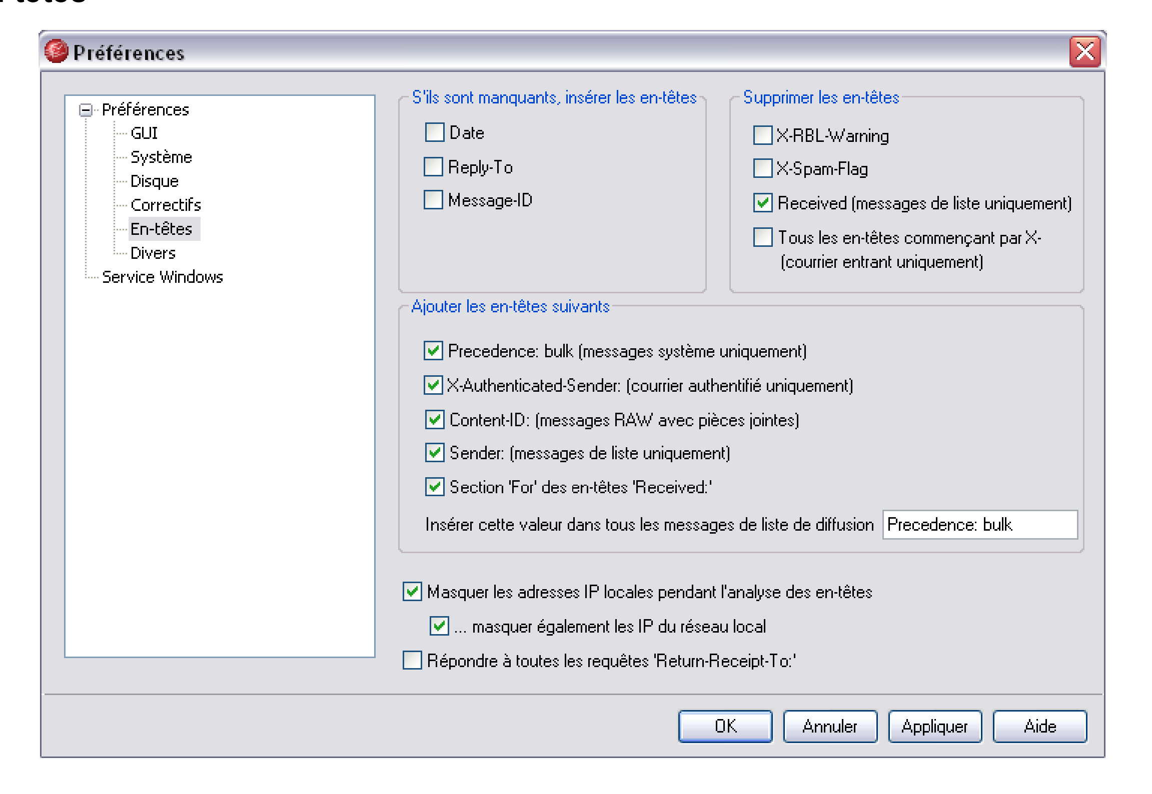
Désactiver la commande IMAP 'IDLE' (déconseillé)
Certains anciens clients de messagerie rencontrent des problèmes avec l'extension `IMAP IDLE`, c'est pourquoi il est possible de désactiver le support de cette extension. Ceci est toutefois déconseillé.

Corriger les en-têtes inexacts en ajoutant le préfixe : “X-MD-Bad-Header:”
Lorsque cette option est activée et que MDaemon rencontre un en-tête inexact, il ajoute le préfixe "`X-MD-Bad-Header:`".

Copier 'Sender:' dans 'From:' si 'From:' est manquant
Certains clients de messagerie ne créent pas d'en-tête FROM lors de la rédaction d'un message, mais placent les informations contenues dans l'en-tête FROM dans l'en-tête SENDER. Cela peut porter à confusion aussi bien pour les serveurs de messagerie en aval que pour le destinataire du message. Activez cette option pour que MDaemon crée l'en-tête FROM manquant à l'aide de l'adresse trouvée dans l'en-tête SENDER.

Accepter le message même si la connexion s'arrête après la commande DATA (peut générer des doublons)
Lorsque cette option est activée, MDaemon accepte et distribue le message même si la connexion est interrompue pendant ou juste après la commande DATA. Cette option ne doit pas être activée dans des conditions normales car elle peut générer des doublons.

3.6.1.5 En-têtes



S'ils sont manquants, insérer les en-têtes

Date
Lorsqu'un message arrive sans en-tête "Date:", MDaemon en crée un nouveau et l'ajoute dans le message si cette option est activée. Il s'agit de la date de réception du message par MDaemon, et non de sa date de création par l'expéditeur. En effet, certains clients de messagerie ne créent pas cet en-tête. Comme certains serveurs n'acceptent pas les messages si cet en-tête est manquant, cette fonctionnalité

permet de les distribuer.

Reply-To
Lorsque cette option est activée et qu'un message arrive sans en-tête "Reply-To", MDaemon en crée un et l'ajoute au message à l'aide de l'adresse trouvée dans l'en-tête "From". Si un en-tête "Reply-To" est présent mais vide, MDaemon crée un en-tête du type Reply-To: "". Cela permet de corriger des problèmes pour certains clients de messagerie.

Message-ID
Lorsqu'un message arrive sans en-tête "Message-ID", MDaemon en crée un au hasard et l'insère dans le message.

Supprimer les en-têtes

X-RBL-Warning
Activez cette option si vous souhaitez supprimer les en-têtes "`X-RBL-Warning:`" trouvés dans les messages. Cette option est désactivée par défaut.

X-Spam-Flag
Activez cette option si vous souhaitez supprimer les anciens en-têtes "`X-Spam-Flag:`" des messages.

Received (messages de liste uniquement)
Activez cette option si vous souhaitez supprimer tous les en-têtes "`Received:`" existants des messages de listes de diffusion.

Tous les en-têtes commençant par X- (courrier entrant uniquement)
MDaemon et les autres serveurs de messagerie utilisent de nombreux en-têtes spécifiques appelés en-têtes "X-Type" afin de router le courrier et d'effectuer de nombreuses fonctions . Lorsque cette option est activée, MDaemon supprime ces en-têtes des messages entrants. **Remarque :** cette option ne supprime pas les en-têtes `X-RBL-Warning`.

Ajouter les en-têtes suivants

Precedence: bulk (messages système uniquement)
Activez cette option si vous voulez qu'un en-tête "Precedence: bulk" soit inséré dans tous les messages générés par le système (messages de bienvenue, avertissement, notifications de non distribution, etc.).

X-Authenticated-Sender: (courrier authentifié uniquement)
Activez cette option si vous voulez que MDaemon ajoute un en-tête "X-Authenticated-Sender:" dans les messages qui arrivent sur une session authentifiée à l'aide de la commande AUTH.

Content-ID: (messages RAW avec pièces jointes)
Activez cette option si vous souhaitez ajouter des en-têtes uniques MIME Content-ID aux messages que MDaemon crée depuis un fichier RAW qui contient des pièces jointes.

Sender: (messages de liste uniquement)
Cochez cette option si vous souhaitez inclure l'en-tête Sender dans les messages des listes de diffusion. Cet en-tête étant requis pour les signatures DomainKeys, l'option ne s'applique pas si MDaemon est configuré pour signer les messages de liste avec DomainKeys (ils contiennent alors tous l'en-tête Sender).

Section 'For' des en-têtes 'Received:'
Activez cette option si vous voulez que les sections "For [SMTP Recipient]" soient ajoutées à l'en-tête de message "Received:" ajouté par MDaemon.

Insérer cette valeur dans tous les messages de liste de diffusion
Si vous souhaitez ajouter une paire en-tête/valeur (comme par exemple "Precedence:bulk") à tous les messages de liste, indiquez-la ici.

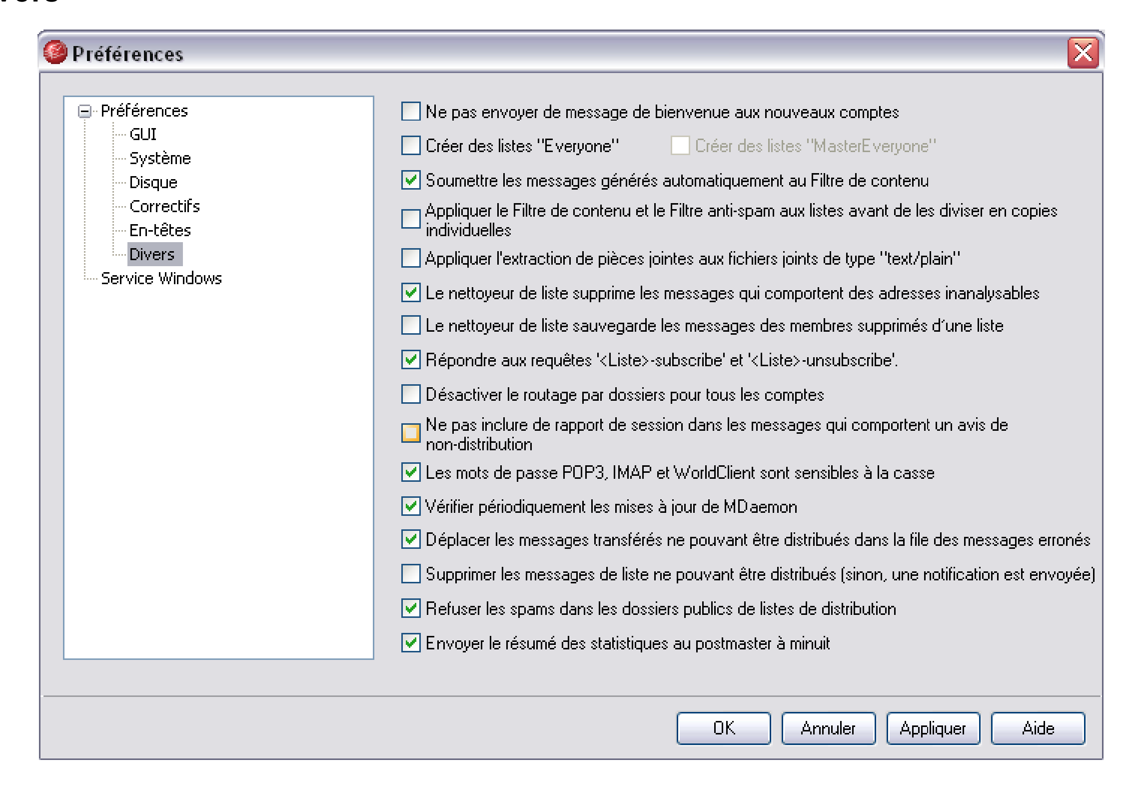
—

Masquer les adresses IP locales pendant l'analyse des en-têtes
Activez cette option pour empêcher MDaemon de placer des adresses IP locales dans les en-têtes de message lorsqu'il traite le courrier.

...masquer également les IP du réseau local (configured in RAS setup)
Lorsque l'option ci-dessus est activée, cochez cette case si vous souhaitez également masquer les adresses IP figurant dans la liste IP LAN 88

Répondre à toutes les requêtes 'Return-Receipt-To:'
Activez cette option pour que les requêtes de confirmation de distribution depuis un message entrant soient honorées. Décochez cette case pour ignorer les requêtes de confirmation de distribution.

3.6.1.6 Divers



Ne pas envoyer de message de bienvenue aux nouveaux comptes
Par défaut, MDaemon génère un message d'accueil basé sur le fichier `NEWUSERHELP.DAT` et l'envoie aux nouveaux utilisateurs lors de la création de leur compte. Activez cette option si vous ne voulez pas que ces messages soient générés.

Créer des listes "Everyone"
Décochez cette case si vous ne souhaitez pas créer et maintenir de liste de diffusion "Everyone" pour vos domaines. En maintenant les listes de diffusion de chaque utilisateur sur chaque domaine MDaemon, vous risquez de gaspiller les ressources si les listes ne sont jamais utilisées ou si elles le sont par un grand nombre d'utilisateurs.

Créer des listes "MasterEveryone"
Activez cette option pour créer une liste de diffusion "MasterEveryone". Tous les membres de toutes les listes "Everyone" seront inclus dans cette liste.

Soumettre les messages générés automatiquement au Filtre de contenu
Cochez cette option si vous souhaitez que tous les messages générés automatiquement (comme les notifications de l'antivirus) soient traités par le Filtre de contenu.

Appliquer le Filtre de contenu et le Filtre anti-spam aux listes avant de les diviser en copies individuelles
Les règles du Filtre de contenu et du Filtre anti-spam s'appliquent aux messages provenant de listes avant qu'ils soient dissociés et distribués aux membres de la liste.

Appliquer l'extraction de pièces jointes aux fichiers joints de type "text/plain"
Par défaut l'extraction automatique de pièces jointes n'extrait pas les fichiers joints de type text/plain. Activez cette option si vous souhaitez les extraire.

Le nettoyeur de liste supprime les messages qui comportent des adresses inanalysables
Lorsque vous avez configuré MDaemon pour qu'il recherche les messages qui sont retournés à une liste de diffusion pour tenter de supprimer les membres de la liste qui ne peuvent être atteints, cette option supprime les messages qui n'ont pas d'adresse pouvant être analysée. Pour plus d'informations, voir l'option *Supprimer automatiquement les adresses non valides de la liste* dans l'onglet Membres de l'Éditeur de liste de diffusion.

Le nettoyeur de liste sauvegarde les messages des membres supprimés d'une liste
Lorsque MDaemon recherche des messages de liste retournés afin de retirer des adresses de membres qui ne peuvent être atteints, cette option enregistre les messages résultant d'un désabonnement d'un membre de la liste.

Répondre aux requêtes'<Liste>-subscribe' et '<Liste>-unsubscribe'
Activez cette option si vous voulez que MDaemon reconnaisse la validité des adresses de ce format (tant que la liste existe) afin de disposer d'une méthode plus simple permettant aux utilisateurs de s'abonner et de se désabonner de vos listes de diffusion. Par exemple, si vous avez une liste nommée MyList@altn.com : les personnes pourront s'abonner/se désabonner de votre liste en envoyant un message à MyList-Subscribe@altn.com et MyList-Unsubscribe@altn.com. Le contenu du sujet et le corps du message n'ont pas d'importance. Ainsi, lorsque cette fonctionnalité est activée, MDaemon insère l'en-tête suivant dans tous les messages de la liste :

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@domain.com>
```

Certains clients de messagerie peuvent l'utiliser et mettre automatiquement un bouton Désinscription à la disposition des utilisateurs.

Désactiver le routage par dossiers pour tous les comptes
Cette option désactive le routage par dossiers de façon globale, quels que soient les paramètres des comptes. Pour en savoir plus sur le routage par dossiers, voir l'onglet Filtres IMAP 307 de l'Éditeur de compte.

Ne pas inclure de rapport de session dans les messages qui comportent un avis de non distribution
Sélectionnez cette option si vous ne voulez pas que des rapports de session SMTP soient inclus dans les messages d'erreur de distribution ou d'avertissement.

Les mots de passe POP3, IMAP et WorldClient sont sensibles à la casse
Activez cette option si vous souhaitez que les mots de passe POP, IMAP et WorldClient respectent la casse.

Vérifier périodiquement les mises à jour de MDaemon
Activez cette option si vous souhaitez que MDaemon recherche régulièrement si une nouvelle version est disponible.

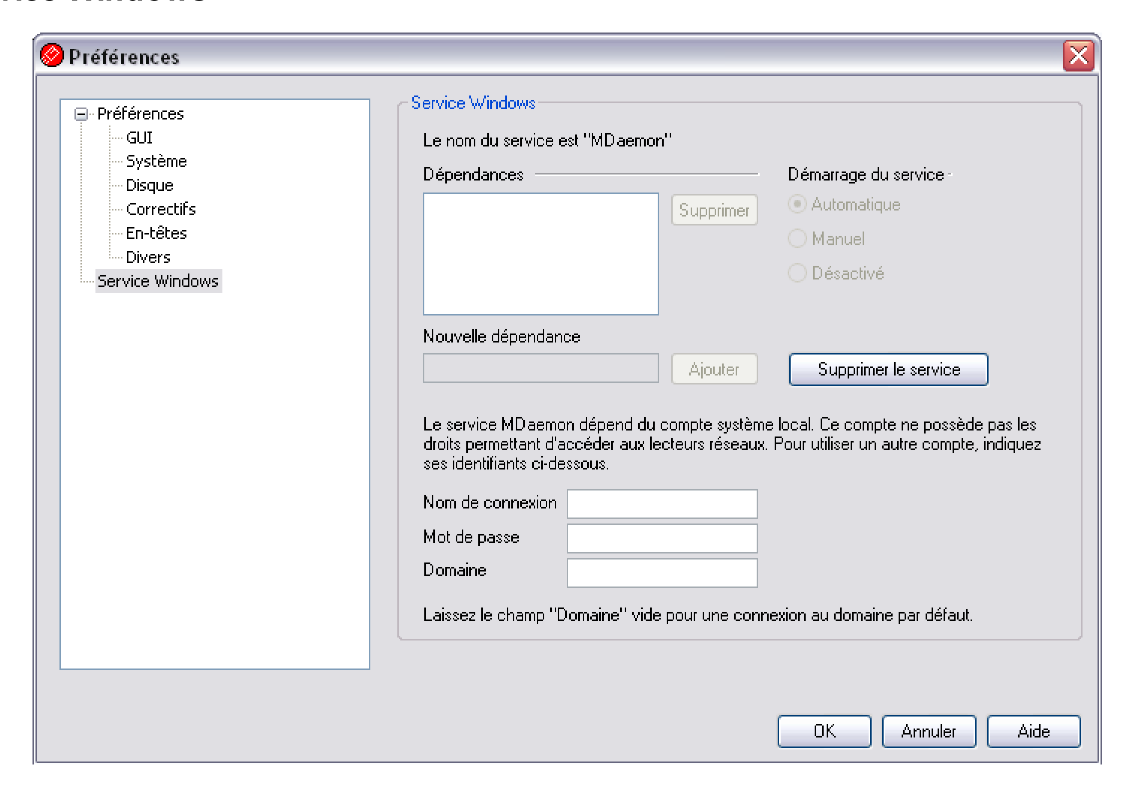
Déplacer les messages transférés ne pouvant être distribués dans la file des messages erronés
Lorsque cette option est activée, les messages transférés générant des erreurs permanentes de distribution ou ayant expiré dans la file de relance sont déplacés dans la file des messages erronés et aucune notification n'est envoyée à l'expéditeur d'origine. Si vous désactivez cette option, une notification de non distribution est envoyée à l'expéditeur d'origine.

Supprimer les messages de liste ne pouvant être distribués (sinon, une notification est envoyée)
Lorsque cette option est activée, les messages de liste générant des erreurs permanentes de distribution ou ayant expiré dans la file de relance sont supprimés, et aucune notification n'est envoyée à l'expéditeur d'origine. When this option is disabled, Si vous désactivez cette option, une notification de non distribution est envoyée à l'adresse *SMTP 'Bounce'* 391 de la liste.

Refuser les spams dans les dossiers publics de listes de diffusion
Par défaut, lorsqu'un dossier public 394 est associé à une liste diffusion, les messages de la liste considérés comme des spams (dont le score est supérieur ou égal à la valeur indiquée dans "*Un message est considéré comme du spam...*" des option du Filtre anti-spam 209) ne sont pas placés dans ce dossier.

Envoyer le résumé des statistiques au postmaster à minuit
Activez cette option si vous souhaitez qu'un rapport sur les statistiques soit envoyé tous les jours au postmaster. Décochez cette case si vous ne souhaitez pas envoyer ce rapport. Le contenu de ce résumé correspond à celui de l'onglet Statistiques 23 de l'interface générale de MDaemon.

3.6.2 Service Windows



Service Windows

Lorsque MDaemon est exécuté en tant que service, le nom du service est "MDaemon".

Dépendances

Liste des services qui doivent être actifs avant le démarrage du service MDaemon.

Démarrage du service

État initial du service : démarrage automatique, manuel, ou service désactivé.

Installer/supprimer le service

Cliquez sur ce bouton pour installer ou supprimer le service MDaemon.

Accès aux ressources réseau

Lorsque vous exécutez MDaemon en tant que service système, il s'exécute par défaut sous le compte système local. Dans la mesure où ce compte n'a pas accès au réseau, MDaemon ne pourra pas accéder au courrier si vous souhaitez le stocker sur d'autres ordinateurs de votre réseau local. Par contre, vous pouvez en cas de besoin créer un compte Windows et lui fournir des identifiants qui permettront au service MDaemon d'accéder aux partages réseau. Les applications lancées par MDaemon (par exemple, les utilitaires MDStats et Prétraitement) utiliseront également les paramètres de sécurité du compte Windows.

Nom de connexion

Il s'agit du nom de connexion du compte Windows utilisé par le service MDaemon.

Mot de passe
Mot de passe du compte Windows.

Domaine
Domaine Windows sur lequel se trouve le compte. Laissez ce champ vide pour vous connecter au domaine par défaut.



Section IV

4 Menu Sécurité

MDaemon est doté d'une suite complète de fonctionnalités et d'options de sécurité. Cliquez sur Sécurité dans la barre de menus de MDaemon pour accéder aux fonctionnalités de sécurité suivantes :

- **Antivirus** 177 — SecurityPlus for MDaemon est la meilleure protection intégrée existante mise à disposition des clients de MDaemon. Cette application permet de bloquer les virus acheminés par message électronique : elle détecte, met en quarantaine, répare et/ou détruit les messages électroniques qui contiennent un virus. SecurityPlus contient également une fonctionnalité appelée Protection instantanée, disponible uniquement avec MDaemon Pro. Elle protège contre certaines attaques de spams, phishing ou virus n'étant pas toujours détectées par les outils de protection traditionnels.
- **Filtre de contenu** 178 — Un système de filtrage de contenu totalement polyvalent et multiprocessus vous permet de personnaliser le comportement du serveur à partir du contenu du courrier entrant et sortant. Vous pouvez insérer et supprimer des en-têtes de messages, ajouter des pieds de pages aux messages, supprimer des pièces jointes, envoyer des copies ou un message instantané à des utilisateurs, exécuter des programmes, et bien d'autres fonctions encore.
- **Filtre anti-spam** 208 — Une technologie de filtrage du spam permet d'analyser et d'attribuer un « score » au courrier électronique à l'aide du moteur heuristique. Le score sert à évaluer la probabilité pour qu'un message soit du spam. Le serveur agira ensuite selon ce résultat, en refusant ou en marquant de message par exemple. Voir également : Pièges à spam 237.
- **Listes noires DNS** 231 — Cette fonctionnalité vous permet d'indiquer plusieurs services de listes noires DNS qui seront consultés chaque fois que quelqu'un essaie d'envoyer un message à votre serveur. Si l'IP qui se connecte figure sur la liste noire de l'un de ces hôtes, le message sera refusé ou marqué.
- **Paramètres de relais** 238 — Ces paramètres permettent de déterminer ce que MDaemon fera d'un message qui arrive sur votre serveur et ne provient pas ou n'est pas destiné à une adresse locale.
- **Bouclier IP** 240 — Si un nom de domaine indiqué dans cette liste tente de se connecter à votre serveur, son adresse IP doit correspondre à celle que vous lui avez attribuée.
- **Authentification SMTP** 247 — Cette fonction sert à définir plusieurs options déterminant le comportement de MDaemon selon que l'expéditeur d'un message au serveur a été authentifié ou pas.
- **Vérifications inverses** 242 — MDaemon peut interroger des serveurs DNS pour vérifier la validité des noms de domaines et des adresses indiqués lors de l'arrivée de messages. Les commandes de cet onglet peuvent être utilisées pour que les messages suspects soient refusés ou qu'un en-tête spécial y soit inséré. Les données de la vérification inverse seront également enregistrées dans les fichiers journaux de MDaemon.
- **POP avant SMTP** 245 — Les commandes de cet onglet servent à exiger de chaque utilisateur qu'il accède d'abord à sa boîte aux lettres avant d'être

autorisé à envoyer un message via MDaemon. Cela permet de vérifier que l'utilisateur est titulaire d'un compte valide et qu'il est peut utiliser le système de messagerie.

- **Hôtes autorisés** 246 — Il s'agit des adresses IP et domaines qui seront considérés comme des exceptions aux règles de renvoi.
- **SPF/Sender ID** 249 — Tous les domaines publient des enregistrements MX permettant d'identifier les machines susceptibles de recevoir leurs messages, mais pas celles pouvant en envoyer. Avec le SPF (Sender Policy Framework) et Sender ID, les domaines peuvent également publier des enregistrements MX « inversés », afin d'identifier les postes autorisés à envoyer des messages.
- **DomainKeys et DomainKeys Identified Mail** 251 — DomainKeys et DKIM sont des systèmes de vérification du courrier possédant de nombreuses fonctionnalités : lutte contre le « spoofing » (usurpation d'adresse), vérification de l'intégrité des messages entrants (qu'ils n'aient pas été altérés au cours du transfert entre les serveurs). Ils fonctionnent à l'aide d'un système de paires de clés cryptées publiques et privées. Les messages sortants sont signés avec une clé privée et les messages entrants vérifiés avec la clé publique correspondante publiée sur le serveur DNS de l'expéditeur.
- **Certification** 260 — La certification des messages est un procédé par lequel des fournisseurs de services de certification se "portent garants" de la bonne conduite de l'expéditeur d'un message. Par conséquent, les messages envoyés depuis un domaine pour lequel un fournisseur de certification se porte garant peuvent être plus facilement considérés comme légitimes. La certification permet d'éviter que des messages soient soumis inutilement au Filtre anti-spam et diminue les ressources nécessaires pour le traitement de chaque message.
- **Liste noire d'adresses** 265 — Listes d'adresses n'étant pas autorisés à utiliser votre serveur.
- **Écran IP** 266 — L'écran IP sert à désigner les adresses IP qui sont autorisées ou non à se connecter à votre serveur.
- **Écran d'hôte** 268 — L'écran d'hôte sert à désigner les hôtes (noms de domaine) qui sont autorisés ou non à se connecter à votre serveur.
- **Écran dynamique** 269 — Avec l'Écran dynamique, MDaemon analyse le "comportement" des serveurs lui envoyant du courrier. Par exemple, il est possible de refuser temporairement les connexions d'une adresse IP si le nombre d'erreurs "destinataire inconnu" au cours de la session est trop important. De même, vous pouvez bloquer les IP qui se connectent trop souvent à votre serveur au cours d'une période définie, ainsi que celles dont l'authentification échoue un nombre de fois supérieur à celui indiqué.
- **SSL & TLS** 271 — MDaemon supporte le protocole SSL (Secure Sockets Layer)/ TLS (Transport Layer Security) pour SMTP, POP, IMAP, WebAdmin et WorldClient. SSL est la méthode standard qui permet de sécuriser les communications Internet entre le serveur et le client.
- **Protection contre les retours de courrier** 283 — Les "retours de courrier" sont des messages que les utilisateurs reçoivent en réponse à des e-mails qu'ils n'ont jamais envoyés. Cela se produit lorsque des spams ou virus sont envoyés avec une adresse de retour (valeur "Return-path") usurpée. Lorsque l'un de ces messages est rejeté par le serveur du destinataire, ou si le compte a activé un

autorépondeur ; la réponse est envoyée à l'adresse usurpée. Le propriétaire de l'adresse reçoit alors des centaines de notifications, messages d'absence, etc., non sollicités. De plus, des spammeurs ou personnes malintentionnées profitent souvent de ce phénomène pour lancer des attaques DoS (Denial of Service) contre les serveurs de messagerie.

- **Régulation de la bande passante** 286 — La Régulation de la bande passante permet de maîtriser l'utilisation de la bande passante par MDaemon. Vous pouvez contrôler le taux de progression des sessions et services ; des taux différents peuvent être fixés par domaine (y compris pour le domaine par défaut, les domaines supplémentaires et les passerelles) pour les principaux services de MDaemon.
- **Paramètres de répulsion** 288 — La répulsion vous permet de retarder volontairement une connexion lorsqu'un nombre précis de commandes RCPT ont été envoyées par un même expéditeur. Cette fonction vise à dissuader les spammeurs d'utiliser votre serveur pour envoyer en masse du courrier non souhaité (« spam »). En effet, la durée d'envoi de chaque message est allongée de façon excessive, ce qui décourage les spammeurs de se servir à nouveau de votre serveur
- **Liste grise** 290 — La liste grise est une technique de lutte contre le spam consistant à renvoyer une erreur temporaire aux serveurs SMTP envoyant du courrier à MDaemon afin qu'ils renouvellement la tentative ultérieurement. Ainsi, les messages reçus d'un expéditeur inconnu ou ne figurant pas sur la liste blanche sont temporairement refusés au cours de la session SMTP, et le destinataire et l'adresse IP de l'expéditeur sont enregistrés. De plus, toute tentative de distribution de cet expéditeur sera également refusée pendant une période définie. Cette méthode a pour but de réduire le nombre de spams reçus par les utilisateurs, car les spammeurs ne renouvellent généralement pas les tentatives d'envoi lorsqu'un message est refusé.
- **HashCash** 293 — HashCash est un système d'affranchissement électronique permettant à la fois de lutter contre le spam et les attaques par déni de service. Il génère des timbres virtuels ("payés" avec du temps processeur), qui sont insérés dans les en-têtes des messages sortants puis vérifiés par le serveur du destinataire. Les messages comportant un timbre ont donc de fortes chances d'être légitimes, c'est pourquoi ils sont acceptés par les systèmes anti-spam. Le système HashCash réduit le nombre de faux positifs et évite que certains messages soient rejetés par erreur par des filtres ou des listes noires.
- **IP LAN** 295 — Cette liste contient les adresses IP de votre réseau local (LAN). Ces IP sont donc considérées comme locales par le système de régulation de la bande passante. De plus, plusieurs autres restrictions concernant la sécurité et les mesures de prévention du spam ne sont pas appliquées à ces adresses.
- **Politique du site** 296 — sCette fonction permet de créer une politique de sécurité du site qui est transmise aux serveurs d'envoi au début de chaque session SMTP. « Ce serveur n'est pas un relais » est un exemple de politique de site couramment utilisée.

4.1 Filtre de contenu et antivirus

Filtre de contenu

Le Filtre de contenu[178] (Sécurité » Filtre de contenu) permet d'automatiser de nombreuses actions : blocage des spams, blocage des messages contenant des virus avant qu'ils n'atteignent leur destinaire, copies de certains messages à un ou plusieurs utilisateurs supplémentaires, ajout de texte au bas des messages, ajout/suppression d'en-têtes, suppression de pièces jointes, et bien plus encore. Comme les règles individuelles de Filtre de Contenu sont créées par l'administrateur, et en raison de leur diversité, elles peuvent être utilisées dans de nombreuses situations et ne sont limitées, pour la plupart d'entre elles, que par l'inventivité de leur créateur. Avec un peu de réflexion et de pratique, cette fonctionnalité peut être particulièrement utile.

SecurityPlus for MDaemon



Le module additionnel SecurityPlus for MDaemon s'intègre parfaitement dans MDaemon. Alt-N Technologies, en collaboration avec Kaspersky Labs, développeur de logiciels anti-virus de renommée mondiale, a développé SecurityPlus for MDaemon, un moteur antivirus qui peut être installé et intégré à MDaemon. Lorsque ce module est installé, deux onglets supplémentaires apparaissent dans la boîte de dialogue du Filtre de contenu : Antivirus[197] et Mises à jour antivirus[200]. Ces onglets servent à contrôler directement les fonctionnalités de ce module d'extension et à indiquer les mesures prises par MDaemon lorsqu'un virus est détecté. SecurityPlus contient également une fonctionnalité appelée Protection instantanée[203], disponible uniquement avec MDaemon Pro. Contrairement aux outils traditionnels, basés sur des signatures ou une analyse heuristique, cette fonctionnalité détecte les spams, phishings et virus dès les premières minutes suivant le début d'une attaque. SecurityPlus for MDaemon est disponible à l'adresse www.altn.com.

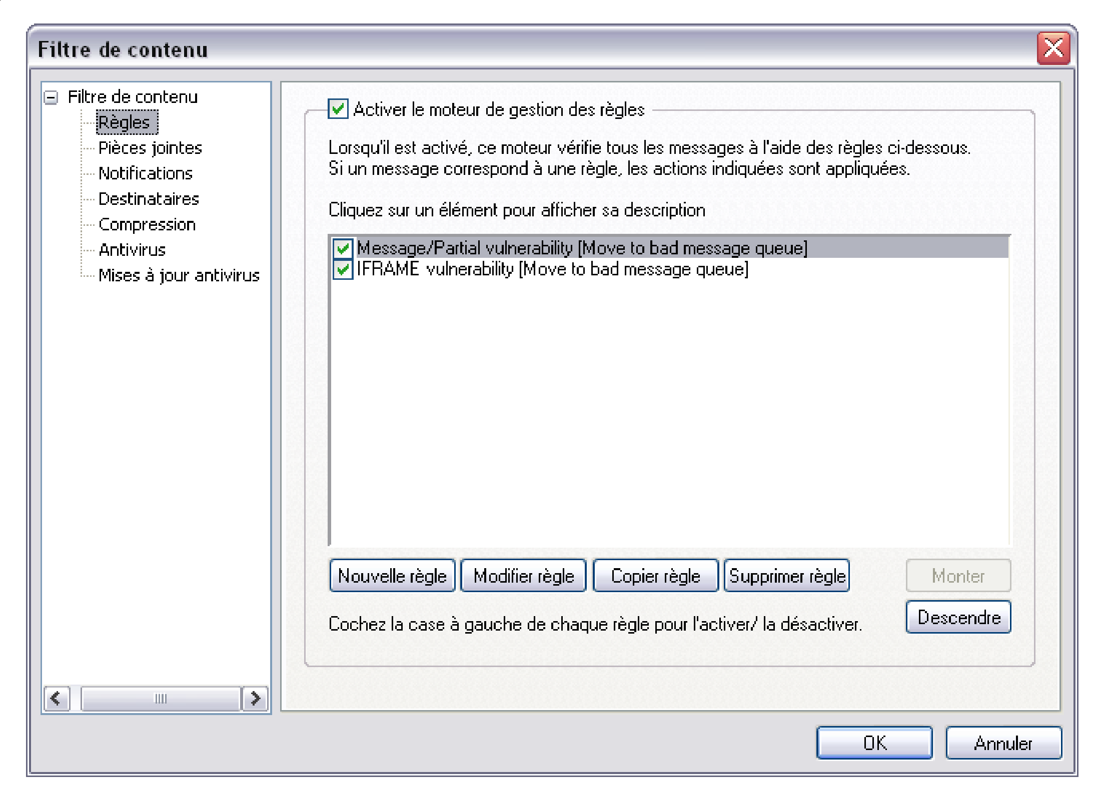
Voir également :

Filtre de contenu 178
Création d'une règle du filtre de contenu 180
Modification d'une règle existante 184
Utilisation d'expressions régulières 184

Antivirus 197
Utilitaire de mise à jour antivirus 200
Protection instantanée 203

4.1.1 Éditeur du Filtre de contenu

4.1.1.1 Règles



Tous les messages traités par MDaemon restent temporairement dans l'une des files d'attente de courrier. Lorsque le filtrage de contenu est activé, avant qu'un message ne soit autorisé à quitter la file d'attente, il est d'abord traité par les règles du Filtre de contenu. Le résultat de cette procédure détermine le sort des messages.



Les messages dont le nom de fichier commence par la lettre "P" sont ignorés par le filtrage de contenu. Lorsqu'un message a été analysé par le Filtre de contenu, MDaemon remplace la

première lettre du nom du fichier par un “P”. Ainsi, les messages ne sont soumis qu'une seule fois au Filtre de contenu.

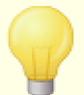
Règles du Filtre de contenu

Activer le moteur de gestion des règles
Cochez cette case pour activer le filtrage de contenu. Tous les messages traités par MDaemon seront filtrés par les règles de filtrage de contenu avant d’être distribués.

Règles existantes

Cette liste contient toutes les règles du Filtre de contenu, précédées d’une case à cocher afin de pouvoir les activer ou les désactiver individuellement. Pour connaître les propriétés d’une règle, cliquez sur nom. Les règles s’appliquent dans l’ordre de la liste. Cela vous permet d’organiser vos règles pour une meilleure flexibilité.

Par exemple, si une règle permet de supprimer tous les messages contenant les mots "Ceci est du spam !", et qu’une autre semblable permette d’envoyer ces messages au Postmaster, en plaçant ces règles dans le bon ordre, elles s’appliqueront toutes les deux à un même message. Cela suppose qu’il n’y ait pas, dans la liste, de règle antérieure "Stop Processing Rules" qui s’applique à ce message. Si c’est le cas, utilisez les boutons Monter/Descendre pour placer la règle "Stop" sous la seconde. Ainsi, chaque message contenant "Ceci est du spam !" sera envoyé en copie au Postmaster, puis supprimé.



MDaemon a la capacité de créer des règles qui effectueront plusieurs tâches et utiliseront la logique et/ou. Par conséquent, en prenant en compte l’exemple ci-dessus, vous pouvez créer une règle unique qui effectuera toutes ces tâches, voire plus.

Nouvelle règle
Cliquez sur ce bouton pour créer une règle de filtrage de contenu. La boîte de dialogue Nouvelle règle 180 s'affiche alors.

Modifier règle
Cliquez sur ce bouton pour ouvrir la règle sélectionnée, dans l'Éditeur de règle 184.

Copier règle
La nouvelle règle portera le nom par défaut "Copy of [Nom de Règle d’origine]". Cela est utile si vous souhaitez créer plusieurs règles similaires. Vous pouvez créer une règle unique, la copier plusieurs fois, puis modifier les copies si cela est nécessaire.

Supprimer règle
Cliquez sur ce bouton pour supprimer la règle de filtrage de contenu sélectionnée. Vous devrez confirmer votre décision avant que MDaemon ne supprime définitivement la règle.

Monter
Cliquez sur ce bouton pour monter la règle sélectionnée dans la liste.

Descendre
Cliquez sur ce bouton pour descendre la règle sélectionnée.

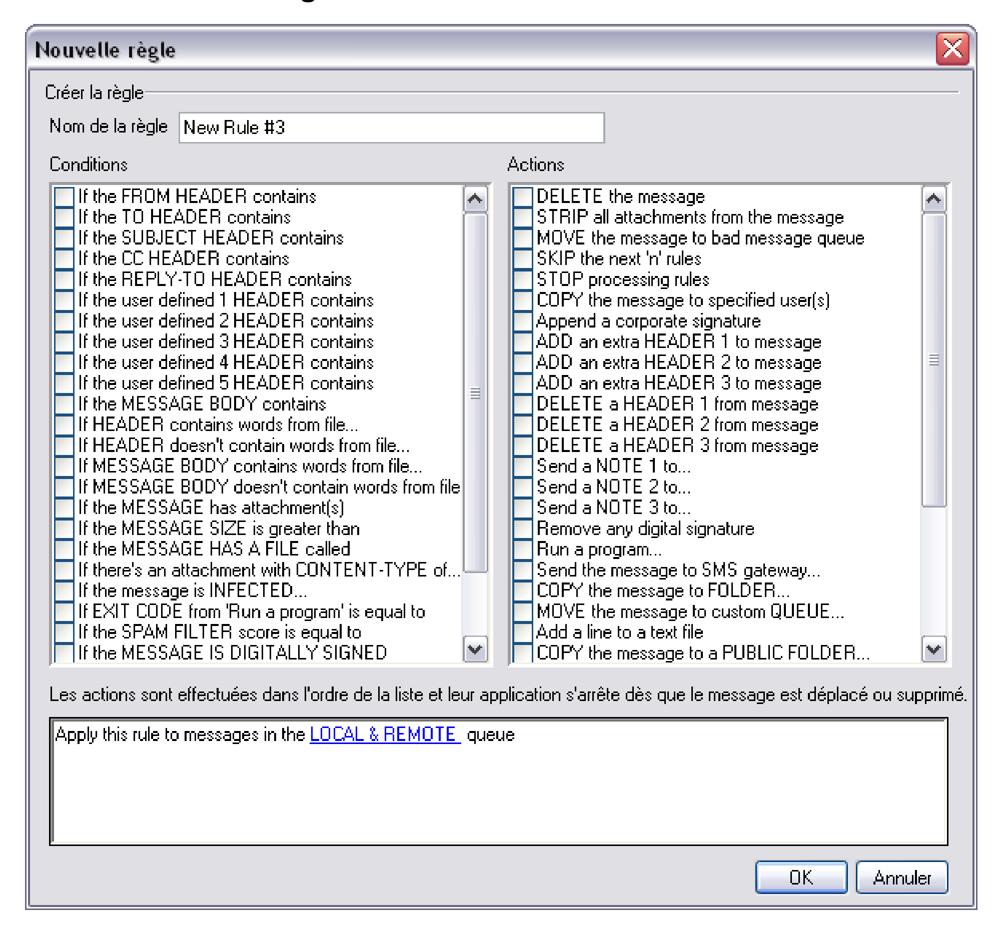
Voir également :

Création d'une nouvelle règle du Filtre de contenu 180

Modification d'une règle existante 184

Utilisation d'expressions régulières 184

4.1.1.1.1 Création d'une nouvelle règle du Filtre de contenu



Cet éditeur permet de créer de nouvelles règles ou de modifier des règles existantes.

Créer la règle

Nom de la règle
Entrez ici un nom descriptif pour la nouvelle règle. Par défaut : New Rule #n.

Conditions...

Cette zone répertorie les conditions qui peuvent s'appliquer à votre nouvelle règle. Cochez les cases correspondant à chacune des conditions que vous souhaitez appliquer à cette règle. Chaque condition sélectionnée apparaîtra dans la zone située en dessous du nom de la règle. La plupart des conditions nécessitent des informations supplémentaires que vous fournirez en cliquant sur le lien hypertexte de chaque condition dans la zone de description de la règle.

If the [HEADER] contains—Cliquez sur l'une de ces options pour que votre règle s'appuie sur le contenu de ces en-têtes de messages précis. Vous devez indiquer le texte à rechercher. Cette condition supporte les expressions régulières 184.

If the user defined [# HEADER] contains—Cliquez sur une ou plusieurs de ces options pour que cette règle s'appuie sur les en-têtes de messages que vous définirez. Vous devez indiquer le nouvel en-tête et le texte à rechercher. Cette condition supporte les expressions régulières 184.

If the MESSAGE BODY contains-Avec cette option, le contenu du corps du message constituera l'une des conditions. Cette condition nécessite que vous indiquiez une chaîne de texte à rechercher. Cette condition supporte les expressions régulières 184.

If the MESSAGE has Attachment(s)—Lorsque cette option est sélectionnée, la règle dépend de la présence d'un ou plusieurs fichiers joints. Aucune information complémentaire n'est nécessaire.

If the MESSAGE SIZE is greater than—Cliquez sur cette option si vous voulez que cette règle soit fondée sur la taille du message. La taille doit être indiquée en Ko. La valeur par défaut est 10Ko.

If the MESSAGE HAS A FILE called—Cette option permet la recherche d'un fichier joint particulier. Vous devez préciser le nom du fichier en question. Les caractères jokers tels que *.exe et fichier*.* sont autorisés.

If message is INFECTED...—Cette condition s'applique lorsque SecurityPlus for MDaemon détermine qu'un message est infecté par un virus.

If the EXIT CODE from a previous run process is equal to —Si une règle précédente dans votre liste contient l'action Run a program..., vous pouvez utiliser cette condition pour rechercher un code de sortie précis dans cette opération.

If the MESSAGE IS DIGITALLY SIGNED—Cette condition s'applique aux messages qui ont été signés numériquement. Aucune information complémentaire n'est requise pour cette condition.

If SENDER is a member of GROUP...—Cette condition s'applique aux messages dont l'expéditeur fait partie du groupe indiqué.

If RECIPIENT is a member of GROUP...—Cette condition s'applique aux messages dont le destinataire fait partie du groupe indiqué.

If ALL MESSAGES —Cliquez sur cette option si vous voulez que la règle s'applique à tous les messages. Aucune information complémentaire n'est nécessaire ; cette règle concernera tous les messages sauf ceux auxquels l'action "Stop Processing Rules", ou "Delete Message" s'applique dans une règle précédente.

Actions...

MDaemon peut effectuer des actions spécifiques lorsqu'un message remplit les conditions de la règle. Certaines actions requièrent des informations complémentaires que vous devez spécifier en cliquant sur le lien hypertexte des actions énumérées dans la zone de description de la règle.

Delete Message—En sélectionnant cette action, les messages correspondant aux conditions indiquées sont supprimés.

Strip All Attachments From Message—Supprime toutes les pièces jointes d'un message.

Move Message To Bad Message Directory—Cette action entraîne le déplacement du courrier vers le dossier des messages erronés.

Skip n Rules—En sélectionnant cette action, un nombre "n" de règles, que vous avez indiqué, est ignoré. Cela est utile lorsque vous souhaitez qu'une règle soit appliquée uniquement dans certains cas.

Par exemple, vous souhaitez supprimer les messages contenant le mot "Spam", mais pas ceux incluant "Faux Spam". Pour cela, vous pouvez créer une règle qui supprime les messages contenant "Spam" et placer, au-dessus, une autre règle qui ignore la première si le message contient "Faux Spam".

Stop Processing Rules—Cette action ignore toutes les règles restantes.

Copy Message To Specified User(s)—Une copie du message est envoyée à un ou plusieurs destinataires. Vous devez préciser les destinataires concernés.

Append Standard Disclaimer—Cette action permet de créer un texte ajouté en pied de page du message. Il possible d'ajouter le contenu d'un fichier texte.

Par exemple, vous pouvez utiliser cette règle pour inclure un texte du type "Ce courrier provient de mon entreprise, contactez moi pour toute réclamation ou question à moi@ma-societe.com".

Add Extra Header Item To Message—Cette action permet d'ajouter un en-tête supplémentaire au message. Vous devez indiquer le nom du nouvel en-tête et son contenu.

Delete A Header Item From Message—Cette action supprime un en-tête d'un

message. Vous devez préciser l'en-tête que vous souhaitez supprimer.

Send Note To... —Cette action entraîne l'envoi d'un message électronique à une adresse spécifique. Vous pouvez indiquer le destinataire, l'expéditeur, le sujet et un texte court. Vous pouvez également configurer cette action pour que le message original soit joint à cette note.

Par exemple, vous pouvez créer une règle qui déplace tous les messages contenant "Ceci est du Spam" vers le dossier de messages erronés, et créer une autre règle qui enverra une note à une personne de votre choix, pour lui signaler cette action.

Remove Digital Signature—Sélectionnez cette action pour qu'une signature numérique soit supprimée du courrier.

Run Process...—Cette action peut être utilisée pour exécuter un programme particulier lorsqu'un message remplit les conditions de la règle. Vous devez indiquer le chemin d'accès au programme que vous souhaitez exécuter. Vous pouvez utiliser la macro $MESSAGEFILENAME$ pour que le nom du message soit traité, et vous pouvez préciser si MDaemon doit suspendre ses opérations, temporairement ou définitivement, lorsqu'il attend la fin du processus. De plus, vous pouvez forcer le programme à s'arrêter et/ou s'exécuter dans une fenêtre masquée.

Send Message Through SMS Gateway Server...—Sélectionnez cette option pour envoyer un message via un serveur de passerelle SMS. Vous devez fournir de nom de l'hôte ou l'adresse IP, ainsi que le numéro du téléphone qui recevra le SMS.

Copy Message to Folder...—Utilisez cette option pour enregistrer une copie du message dans un dossier spécifique.

MOVE the messages to custom QUEUE...—Cette action déplace les messages dans vos files personnalisées. Vous pouvez ensuite créer des programmations personnalisées afin de déterminer les intervalles de traitement de ces messages.

Add Line To Text File—Cette option ajoute une ligne de texte dans un fichier texte spécifique. Lorsque vous choisissez cette option, vous devez indiquer le chemin d'accès au fichier et le texte que vous souhaitez ajouter. Vous pouvez utiliser des macros propres à MDaemon dans votre texte, afin que le Filtre de contenu inclue, de façon dynamique, des informations sur le message telles que l'expéditeur, le destinataire, le code d'identification du message, etc. Cliquez sur le bouton Macros dans la boîte de dialogue Ajouter une ligne au fichier texte pour afficher une liste des macros autorisées.

Move Message to Public Folders...—Utilisez cette action pour que le message soit envoyé vers un ou plusieurs dossiers publics

Search and Replace Words in a Header—Utilisez cette option pour rechercher certains mots dans un en-tête particulier, les supprimer, puis les remplacer. Lorsque vous créez cette règle, cliquez sur le lien "specify information" dans la zone de description de la règle, pour ouvrir la boîte de dialogue En-tête –

Rechercher et Remplacer, dans laquelle vous indiquerez l'en-tête et les mots à remplacer ou à supprimer. Cette action supporte les expressions régulières 184.

Search and Replace Words in the Message Body—Utilisez cette option pour rechercher et remplacer le texte que vous souhaitez dans le corps d'un message. Cette action supporte les expressions régulières 184.

Jump to Rule...—Utilisez cette action pour passer immédiatement d'une règle à une autre dans la liste, en ignorant les règles intermédiaires.

Sign with DomainKeys selector...—Utilisez cette action pour attribuer une signature DomainKeys au message. Elle permet également de signer certains messages avec un sélecteur autre que celui défini dans la boîte de dialogue DomainKeys/DKIM.

Sign with DKIM selector...—Utilisez cette action pour attribuer une signature DKIM 255 au message. Elle permet également de signer certains messages avec un sélecteur autre que celui défini dans la boîte de dialogue DomainKeys/DKIM.

Description de la règle
Cette zone de texte affiche la nouvelle règle sous forme de script. Cliquez sur l'une des conditions ou actions de la règle (lien hypertexte), pour que l'éditeur approprié s'ouvre et ainsi indiquer les informations requises.

Voir :

Éditeur du filtre de contenu 178
Modification d'une règle existante 184
Utilisation d'expressions régulières 184

4.1.1.1.2 Modification d'une règle existante

Pour modifier une règle de Filtre de contenu existante, sélectionnez-la, puis cliquez sur le bouton *Modifier règle*, dans la boîte de dialogue Filtre de contenu. Cette règle s'affichera dans l'éditeur de modification de règle pour pouvoir être modifiée. Les commandes de cet éditeur sont identiques à celles de la boîte de dialogue Création d'une nouvelle règle 180.

Voir également :

Éditeur de Filtre de contenu 178
Modification d'une règle existante 184
Utilisation d'expressions régulières 184

4.1.1.1.3 Expressions régulières

Le système de Filtre de contenu supporte également les recherches d' "expressions

régulières". Ce système permet de rechercher des *modèles* de texte. Les expressions régulières contiennent à la fois du texte en clair et des caractères spécifiques qui indiquent le type de correspondance à effectuer. Cela rend vos règles de Filtre de contenu plus efficaces et précises.

Que sont les expressions régulières ?
Une expression régulière (regexp) est un modèle de texte composé d'une association de caractères spécifiques, appelés métacaractères, et de caractères alphanumériques, ou "littéraux" (abc, 123, etc.). Le modèle sert à trouver des correspondances dans la chaîne de texte. Les expressions régulières sont utilisées principalement pour chercher et remplacer des correspondances avec du texte.

Les métacaractères sont des caractères spéciaux qui possèdent des fonctions particulières dans les expressions régulières. MDaemon accepte les métacaractères suivants :

```
\ | () [] ^ $ * + ? . <>
```

<table>
<tr><th>Métacaractère</th><th>Description</th></tr>
<tr><td>\</td><td>Si vous utilisez la barre oblique inverse ("\") devant un métacaractère, ce dernier sera traité comme un caractère littéral. Cela est nécessaire si vous voulez que l'expression régulière cherche l'un des caractères spéciaux utilisés en tant que métacaractères. Par exemple, pour chercher le signe "+", votre expression doit inclure "\+".</td></tr>
<tr><td>|</td><td>Le caractère "|" s'utilise lorsque vous souhaitez qu'une expression, située à côté de ce caractère, trouve une correspondance de la chaîne cible. L'expression régulière "abc|xyz" trouvera toutes les occurrences, à la fois de "abc" et de "xyz" lors de la recherche d'une chaîne de texte.</td></tr>
<tr><td>[...]</td><td>Si un ensemble de caractères est inclus entre crochets, cela signifie que tous ces caractères doivent correspondre à la chaîne de texte recherchée. Les séries de caractères entre crochets sont séparées par des tirets ("-"). Par exemple, la recherche de la chaîne "abc" avec l'expression régulière "[a-z]" donnera trois correspondances : "a", "b" et "c". En utilisant l'expression "[az]", une seule correspondance sera trouvée : "a".</td></tr>
<tr><td>^</td><td>Ce caractère indique le début d'une ligne. Dans la chaîne cible "abc ab a", l'expression "^a" donnera lieu à une correspondance : le premier caractère de la chaîne cible. L'expression régulière "^ab" donnera également une correspondance : les deux premiers caractères de la chaîne cible.</td></tr>
<tr><td>[^...]</td><td>Ce caractère placé après le crochet gauche possède un sens différent. Il est utilisé pour exclure de la chaîne cible,</td></tr>
</table>

les autres caractères inclus entre crochets. L'expression "[^0-9]" indique que le caractère cible ne doit pas être un chiffre.

(...) La parenthèse indique l'ordre d'évaluation du modèle. Elle sert aussi d'expression marquée pouvant être utilisée dans les expressions chercher et remplacer.

Les résultats d'une recherche, effectuée avec une expression régulière, sont conservés temporairement et peuvent être utilisés dans l'expression remplacer pour créer une autre expression. Dans l'expression remplacer, il est possible d'inclure un caractère "&" ou "\0" qui sera remplacé par la sous-chaîne trouvée par l'expression régulière lors de la recherche. Ainsi, si l'expression chercher "a(bcd)e" trouve une correspondance de sous-chaîne, une expression remplacer "123-&-123" ou "123-\0-123" remplacera le texte trouvé par "123-abcde-123".

De même, vous pouvez utiliser les caractères spéciaux "\1", "\2", "\3", etc. dans l'expression remplacer. Ces caractères seront remplacés par les résultats de l'expression marquée, au lieu de la totalité de la sous-chaîne. Le nombre qui suit la barre oblique inversée détermine l'expression marquée que vous voulez référencer (dans le cas d'une expression régulière contenant plus d'une expression marquée). Par exemple, si l'expression chercher est « (123)(456) et que votre expression remplacer est « a-\2-b\1 », une sous-chaîne sera alors remplacée par « a-456-b-123 », tandis qu'une expression remplacer « a-\0-b » sera remplacée par « a-123456-b ».

**$** Le symbole dollar ("$") indique la fin de la ligne. Dans la chaîne de texte "13 321123", l'expression "3$" donne lieu à une correspondance : le dernier caractère de la chaîne. L'expression régulière "123$" donnera également une correspondance : les trois derniers caractères de la chaîne cible.

***** L'astérisque ("*") indique que le caractère situé à sa gauche doit correspondre à aucune ou plusieurs occurrences du caractère dans une rangée. Ainsi, "1*abc" correspondra aux textes "111abc" et "abc".

+ Semblable à l'astérisque, le symbole "+" indique que le caractère à sa gauche doit correspondre à une ou plusieurs occurrences du caractère dans une rangée. Ainsi, "1*abc" correspondra au texte "111abc" mais pas à "abc".

? Le point d'interrogation ("?") indique que le caractère à sa gauche doit correspondre à aucune ou une seule correspondance. Ainsi, "1?abc" correspondra au texte

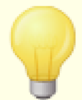
"abc", et à la partie "1abc" de "111abc".

.	Le métacaractère qui représente un point (".") correspondra à n'importe quel caractère. Ainsi, ".+abc" correspondra à "123456abc", et "a.c" correspondra à "aac", "abc", "acc", etc.

Conditions et actions concernées

Les expressions régulières peuvent être utilisées dans toutes les conditions du Filtre de contenu relatives aux en-têtes comme, par exemple, toute règle qui utilise la condition "if the FROM HEADER contains". Les expressions régulières peuvent également être utilisées dans la condition "if the MESSAGE BODY contains".

Les expressions régulières peuvent être utilisées dans deux actions du Filtre de contenu : "Search and Replace Words in a Header" et "Search and Replace Words in the Message Body".



Les expressions régulières utilisées dans les conditions du Filtre de contenu sont sensibles à la casse.

La sensibilité à la casse dans les expressions régulières, utilisées dans les actions du Filtre de contenu, est facultative. Lorsque vous créez une expression dans les actions de la règle, vous pouvez choisir d'activer ou de désactiver la sensibilité à la casse.

Paramétrer une expression régulière dans une condition

Pour paramétrer l'utilisation d'une expression régulière dans une condition relative à un en-tête ou au corps d'un message :

1. Dans la boîte de dialogue Créer une règle, cochez la case qui correspond à la condition relative à l'en-tête ou au corps du message, que vous souhaitez ajouter à la règle.

2. Dans la zone de description située en bas de la boîte de dialogue Créer une règle, cliquez sur le lien *contains specific strings* qui correspond à la condition que vous venez de sélectionner. La boîte de dialogue *Texte à rechercher* s'ouvre.

3. Cliquez sur le lien *contains* dans la zone *Chaînes à vérifier*.

4. Sélectionnez *Matches Regular Expression* dans la liste déroulante, puis cliquez sur OK.

5. Si vous avez besoin d'aide pour créer votre expression régulière, ou que vous souhaitez la tester, cliquez sur le bouton *Tester l'expression régulière*. Si vous ne voulez pas utiliser cette boîte de dialogue pour tester l'expression, saisissez votre expression régulière dans la zone de texte appropriée, cliquez sur Ajouter, puis passez à l'étape 8.

6. Entrez votre expression régulière dans la zone de texte *Texte à rechercher*. Pour simplifier le processus, il existe un menu de raccourcis que vous pouvez utiliser pour insérer facilement les métacaractères de votre choix dans votre expression régulière. Cliquez sur le bouton ">" pour accéder à ce menu. Le métacaractère correspondant à l'option choisie dans ce menu sera inséré dans l'expression, et le point d'insertion du texte sera déplacé à l'endroit associé au caractère.

7. Entrez, dans la zone correspondante, le texte que vous voulez utiliser pour tester votre expression, puis cliquez sur Tester. Lorsque le test est terminé, cliquez sur OK.

8. Cliquez sur OK.

9. Continuez normalement la création de la règle.

Paramétrer une expression régulière dans une action

Pour paramétrer l'utilisation d'une expression régulière dans une action Search and replace :

1. Dans la boîte de dialogue Créer une règle, cochez la case qui correspond à l'action Search and replace… que vous voulez ajouter à la règle.

2. Dans la zone de description située en bas de la boîte de dialogue Créer une règle, cliquez sur le lien *specify information* qui correspond à l'action que vous venez de sélectionner. La boîte de dialogue Chercher et remplacer s'ouvre.

3. Si vous avez choisi l'action Search and replace within header à l'étape 1, choisissez, dans la liste déroulante, l'en-tête que vous voulez chercher, ou, s'il n'y est pas, entrez-le dans la zone de texte. Sinon, passez à l'étape suivante.

4. Saisissez l'expression que vous souhaitez rechercher dans cette action. Pour simplifier le processus, il existe un menu de raccourcis que vous pouvez utiliser pour insérer facilement les métacaractères de votre choix dans votre expression régulière. Cliquez sur le bouton ">" pour accéder à ce menu. Le métacaractère correspondant à l'option que vous aurez choisie dans ce menu sera inséré dans l'expression, et le point d'insertion du texte sera déplacé à l'endroit associé au caractère.

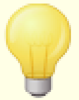
5. Saisissez dans le champ Remplacer par l'expression que vous souhaitez utiliser dans cette action. Comme pour l'expression chercher, il existe un menu de raccourcis pour choisir les métacaractères à insérer dans cette option. Ne remplissez pas ce champ si vous souhaitez que l'expression recherchée soit supprimée et non remplacée par une autre.

6. Cochez la case Expression exacte pour que l'expression soit sensible à la casse.

7. Cochez Expression régulière pour que les chaînes à chercher et à remplacer soient traitées comme des expressions régulières. Sinon, elles seront traitées comme de simples correspondances de sous-chaînes et seront remplacées. La recherche s'effectuera sur une correspondance littérale exacte du texte, au lieu de traiter les chaînes comme des expressions régulières.

8. Si vous n'avez pas besoin de tester votre expression, passez à l'étape suivante. Dans le cas contraire, cliquez sur Test. Dans la boîte de dialogue Test de la fonction : Rechercher et remplacer, saisissez les expressions à chercher et à remplacer, ainsi que le texte à tester, puis cliquez sur le bouton Tester. Lorsque le test des expressions régulières est terminé, cliquez sur OK.

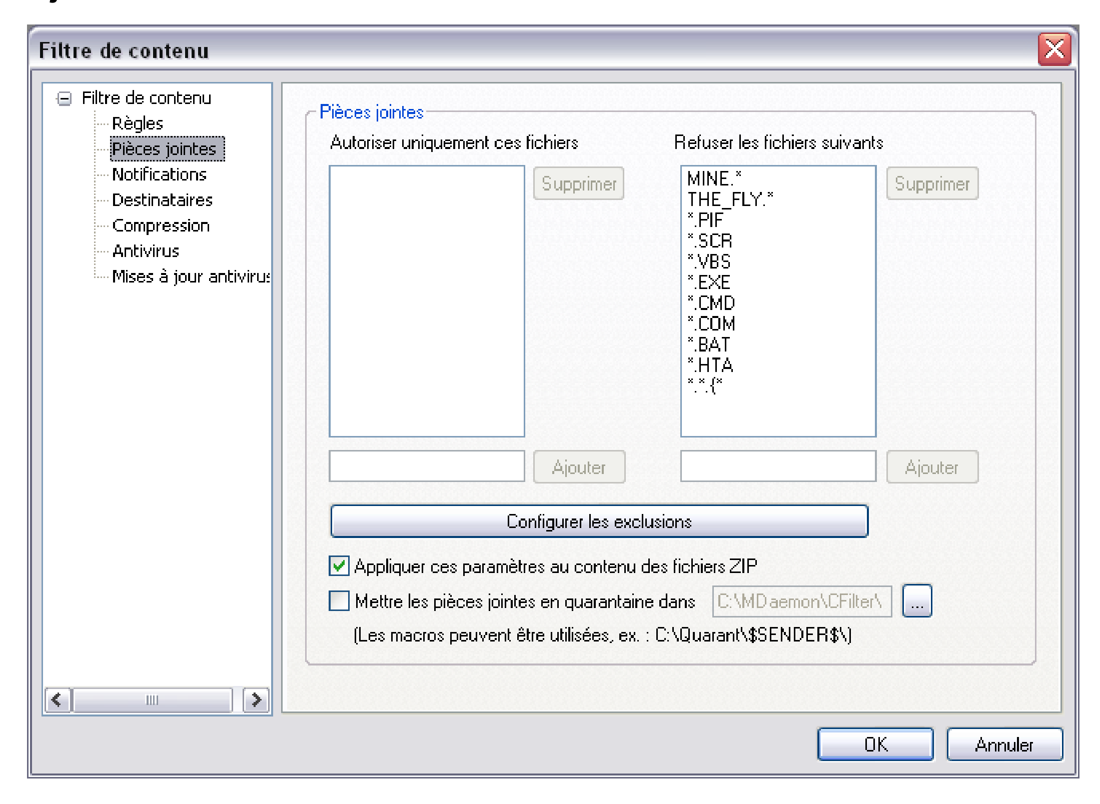
9. Continuez normalement la création de la règle.



MDaemon utilise la librairie PRCE (PERL Compatible Regular Expression). Plus d'informations sur cette implémentation sont disponibles sur les sites : http://www.pcre.org/ et http://perldoc.perl.org/perlre.html (en anglais).

Pour en savoir plus sur les expressions régulières, consultez : *Mastering Regular Expressions, Third Edition* publié par O'Reilly Media, Inc (en anglais).

4.1.1.2 Pièces jointes



Utilisez cet onglet pour indiquer les pièces jointes que vous souhaitez autoriser ou interdire. Les pièces jointes non autorisées sont supprimées automatiquement des messages.

Pièces jointes

Les fichiers indiqués dans la liste *Refuser les fichiers suivants* sont supprimés automatiquement des messages lorsque MDaemon les rencontre. Si vous répertoriez des fichiers dans la liste *Autoriser uniquement ces fichiers*, ils seront les seuls autorisés. Toutes les autres pièces jointes seront supprimées des messages. Après la suppression d'une pièce jointe, MDaemon poursuivra normalement et distribuera seulement le message. Vous pouvez utiliser les options de l'onglet *Notifications* pour qu'un message de notification soit envoyé aux adresses de votre choix lorsque l'une des pièces jointes interdite est rencontrée.

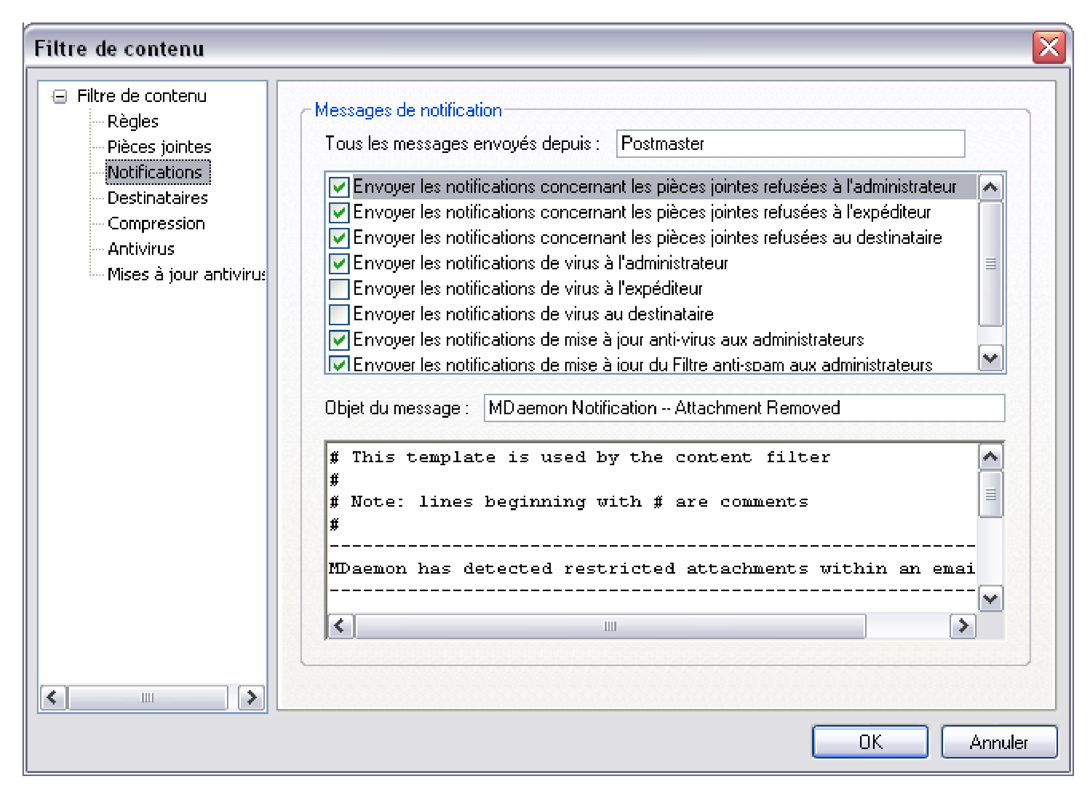
Les caractères jokers sont autorisés dans les entrées de la liste. Une entrée du type "*.exe", par exemple, entraînerait soit l'autorisation, soit la suppression de toutes les pièces jointes avec une extension .EXE. Pour ajouter une entrée à l'une de ces listes, entrez le nom de fichier dans l'espace correspondant, puis cliquez sur *Ajouter*.

Configurer les exclusions
Cliquez sur ce bouton pour indiquer les adresses que vous souhaitez exclure de l'interdiction de pièces jointes. Lorsqu'un message est destiné à l'une de ces adresses, MDaemon autorise le message même s'il contient une pièce jointe interdite.

Appliquer ces paramètres au contenu des fichiers ZIP
Cette option vérifie la présence de pièces jointes interdites dans les fichiers ZIP. De plus, lorsqu'elle est activée les règles basées sur le nom du fichier s'appliquent également aux fichiers inclus dans des ZIP.

Mettre les pièces jointes en quarantaine dans :
Si vous souhaitez que les pièces jointes refusées soient mises en quarantaine au lieu d'être supprimées, activez cette option et indiquez le chemin d'accès du dossier choisi pour les conserver.

4.1.1.3 Notifications



Utilisez cet onglet pour indiquer les personnes qui doivent recevoir des messages de notification lorsqu'un virus ou une pièce jointe interdite sont détectés.

Messages de notification

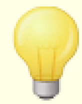
Tous les messages envoyés depuis :
Indiquez dans ce champ l'adresse utilisée pour envoyer les messages de notification.

Envoyer les notifications de virus à...
Lorsqu'un message reçu contient une pièce jointe infectée par un virus, un message d'avertissement est envoyée aux destinataires indiqués ici. Il est possible d'envoyer un message personnalisé aux personnes indiquées dans l'onglet *Destinataires*. Pour personnaliser une notification, sélectionnez une entrée dans la liste, et modifiez le message affiché au-dessous. Il est possible de configurer un message différent pour chaque entrée.

Envoyer les notifications concernant les pièces jointes refusées à...
Lorsqu'un message reçu contient une pièce jointe refusée (voir onglet *Pièces jointes*), un message d'avertissement est envoyée aux destinataires indiqués ici. Il est possible d'envoyer un message personnalisé aux personnes indiquées dans l'onglet *Destinataires*. Pour personnaliser une notification, sélectionnez une entrée dans la liste, et modifiez le message affiché au-dessous. Il est possible de configurer un message différent pour chaque entrée.

Objet du message :
Objet du message de notification envoyé.

Message
Il s'agit du message envoyé aux adresses de l'onglet Destinataires, lorsque la case correspondant à cette entrée est cochée. Vous pouvez modifier directement ce message dans la zone où il est affiché.



Les fichiers contenant ce texte se trouvent dans le répertoire MDaemon\app\. Il s'agit de :

`cfattrem[adm].dat`	Pièce jointe refusée – Admins
`cfattrem[rec].dat`	Pièce jointe refusée – Destinataire
`cfattrem[snd].dat`	Pièce jointe refusée – Expéditeur
`cfvirfnd[adm].dat`	Virus – Admins
`cfvirfnd[rec].dat`	Virus – Destinataire
`cfvirfnd[snd].dat`	Virus – Expéditeur

Si vous souhaitez redonner à l'un de ces messages dans son apparence d'origine, supprimez simplement le fichier concerné, et MDaemon le recréera dans son état par défaut.

4.1.1.3.1 Macros

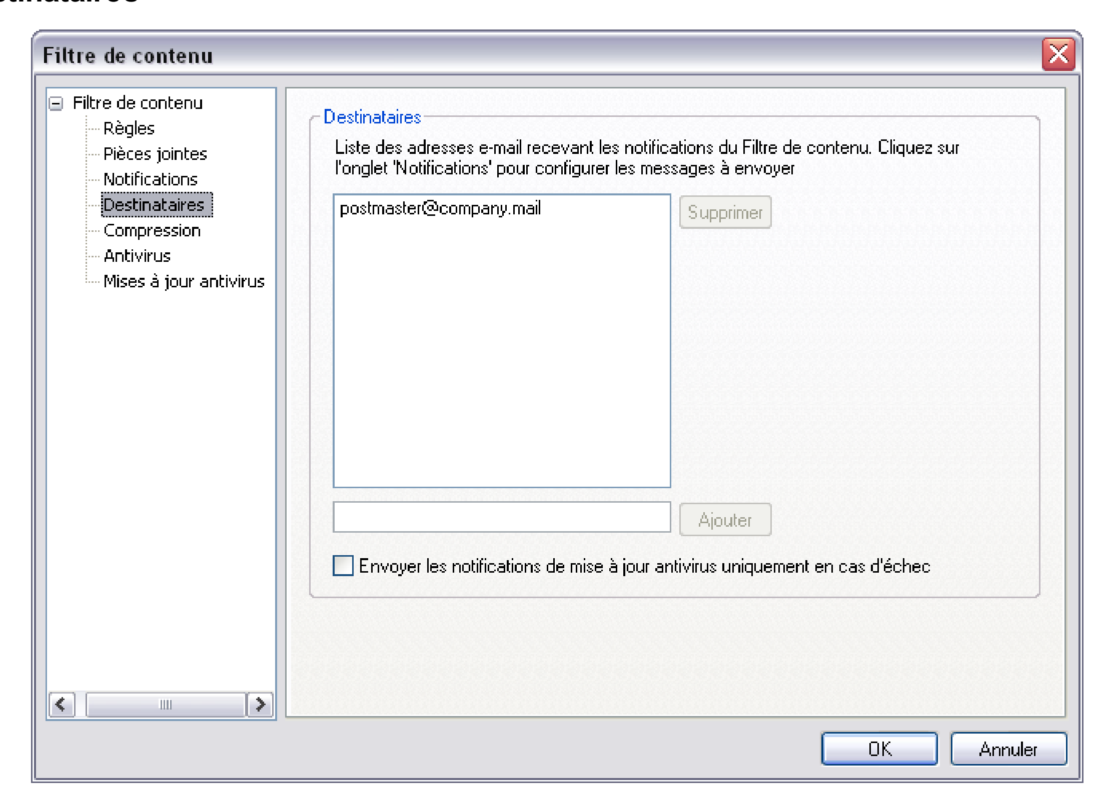
Pour des raisons pratiques, certaines macros peuvent être utilisées dans les messages de notification et les autres messages générés par le Filtre de contenu. Vous pouvez utiliser les macros suivantes :

`$ACTUALTO$`	Certains messages contiennent la macro "ActualTo" remplacée par l'hôte de destination fourni par l'utilisateur d'origine avant chaque reformatage ou conversion d'alias.
`$AV_VERSION$`	Indique la version de SecurityPlus for MDaemon.
`$CURRENTTIME$`	Cette macro est remplacée par l'heure à laquelle le message est traité.
`$ACTUALFROM$`	Certains messages contiennent la macro "ActualFrom" remplacée par l'hôte d'origine avant chaque reformatage ou conversion d'alias.
`$FILTERRULENAME$`	Cette macro est remplacée par le nom de la règle dont les critères ont permis de faire correspondre le message.
`$HEADER:XX$`	Grâce à cette macro, la valeur de l'en-tête indiqué à la place de "xx" sera étendue au message reformaté. Par exemple, si le message d'origine contient "À: joe@mdaemon.com", la macro $HEADER:TO$ s'étendra à

joe@mdaemon.com. Si le message d'origine contient "Objet: Ceci est l'objet", la macro $HEADER:SUBJECT$ sera remplacée par le texte "Ceci est l'objet".

`$HEADER:MESSAGE-ID$`	Comme avec la macro $HEADER:XX$ ci-dessus, cette macro s'étend à la valeur de l'en-tête Message-ID.
`$LIST_ATTACHMENTS_REMOVED$`	Lorsqu'une ou plusieurs pièces jointes sont supprimées d'un message, cette macro les répertorie.
`$LIST_VIRUSES_FOUND$`	Lorsqu'un ou plusieurs virus sont détectés dans un message, cette macro les répertorie.
`$MESSAGEFILENAME$`	Cette macro s'étend au nom de fichier du message en cours de traitement.
`$MESSAGEID$`	Cette macro fonctionne comme $HEADER: MESSAGEID$ ci-dessus, mais elle supprime "<>" de la valeur du numéro d'identification (ID) du message
`$PRIMARYDOMAIN$`	S'étend au nom du domaine par défaut de MDaemon, indiqué dans la boîte de dialogue Domaine par défaut.
`$PRIMARYIP$`	Cette macro s'étend à l'adresse IP de votre domaine par défaut (indiquée dans Configuration > Domaines/Serveurs par défaut).
`$RECIPIENT$`	Cette macro résout l'adresse complète du destinataire du message.
`$RECIPIENTDOMAIN$`	Cette macro insère le nom de domaine du destinataire du message.
`$RECIPIENTMAILBOX$`	Affiche la boîte aux lettres du destinataire (la valeur à gauche du symbole "@" dans l'adresse électronique).
`$REPLYTO$`	Cette macro s'étend à la valeur de l'en-tête "Reply-to" des messages.
`$SENDER$`	S'étend à l'adresse complète depuis laquelle le message a été envoyé.
`$SENDERDOMAIN$`	Cette macro insère le nom de domaine de l'expéditeur du message (la valeur à droite du symbole "@" dans l'adresse électronique).
`$SENDERMAILBOX$`	Affiche la boîte aux lettres de l'expéditeur (la valeur à gauche du symbole "@" dans l'adresse électronique).
`$SUBJECT$`	Affiche le texte contenu dans l'objet du message.

4.1.1.4 Destinataires

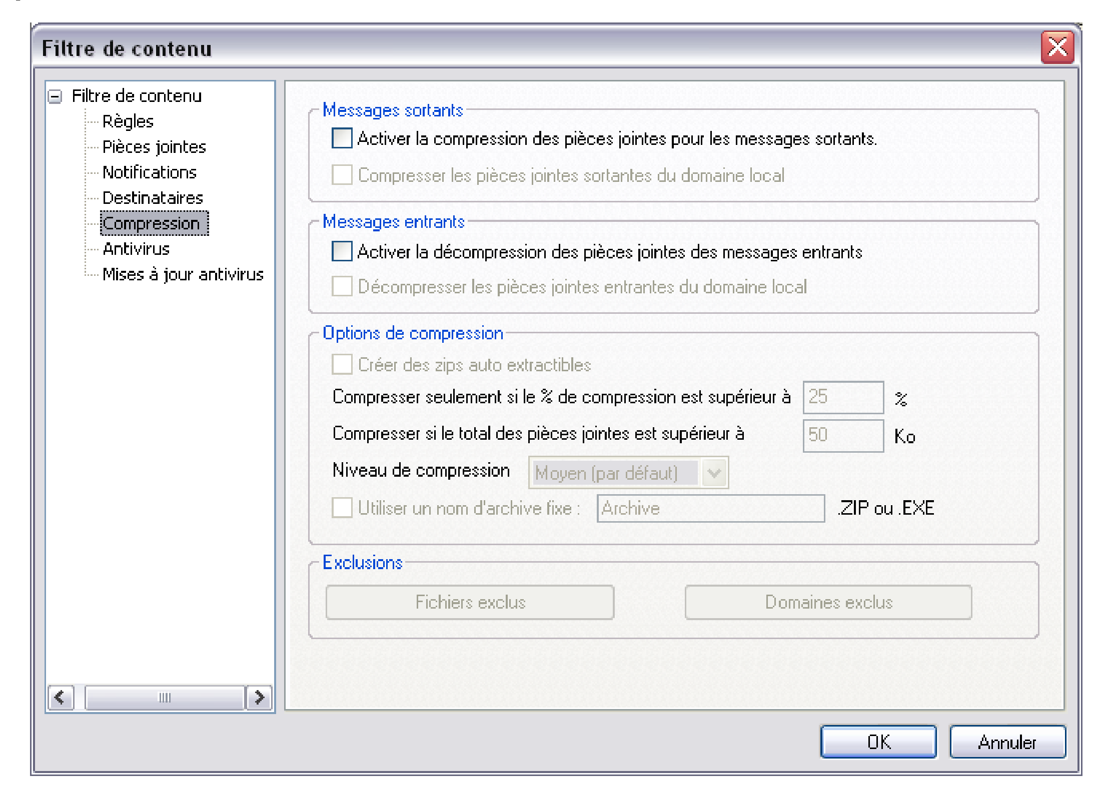


Destinataires

Lorsque l'une des options de l'onglet **Notifications** de type *Envoyer...à l'administrateur* est cochée, les messages de notification sont envoyés aux adresses e-mail figurant dans cette liste. Pour ajouter une adresse, saisissez-la dans l'espace prévu à cet effet puis cliquez sur *Ajouter*. Pour la supprimer, sélectionnez-la et cliquez sur le bouton *Supprimer*.

Envoyer les notifications de mise à jour antivirus uniquement en cas d'échec
Cochez cette option si vous ne souhaitez envoyer les messages de notification de mise à jour antivirus que lorsque la mise à jour échoue.

4.1.1.5 Compression



En utilisant les options de cet onglet, les pièces jointes peuvent être compressées ou décompressées automatiquement avant la distribution d'un message. Il est possible de contrôler le niveau de compression ainsi que plusieurs autres paramètres et exclusions. Cette fonctionnalité réduit de manière significative la bande passante et le débit nécessaires pour la distribution de vos messages sortants.

Messages sortants

Activer la compression des pièces jointes pour les messages sortants
Activez cette option pour activer la compression automatique des pièces jointes des messages distants envoyés à partir du serveur. Le fait de cocher cette option n'entraîne pas la compression de toutes les pièces jointes, mais permet seulement d'activer la fonctionnalité. Ce sont les autres paramètres de cet onglet qui déterminent si les fichiers de messages sortants sont compressés ou non.

Compresser les pièces jointes sortantes du domaine local
En activant cette option, les paramètres de compression de fichiers seront appliqués à tous les messages sortants, même ceux qui sont destinés à une autre adresse locale.

Messages entrants

Activer la décompression des pièces jointes des messages entrants
Activez cette option si vous voulez activer la décompression automatique des pièces jointes des messages distants entrants. Lorsqu'un message qui arrive sur le serveur possède une pièce jointe compressée, MDaemon la décompresse avant

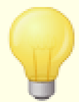
d’envoyer le message à la boîte aux lettres de l’utilisateur local.

Décompresser les pièces jointes entrantes du domaine local
Activez cette option si vous souhaitez que la décompression automatique s’applique également au courrier local.

Options de compression

Créer des zips auto extractibles
Activez cette option si vous voulez que les fichiers de compression créés par MDaemon, soient des fichiers compressés autoextractibles avec une extension .EXE. Cela est utile si les destinataires du message ne disposent pas d’un utilitaire de décompression. Pour décompresser les fichiers compressés autoextractibles, il suffit de double-cliquer dessus.

Compresser seulement si le % de compression est supérieur à xx %
MDaemon ne compresse pas les pièces jointes d’un message avant de l’envoyer sauf si elles peuvent l’être à un pourcentage supérieur à la valeur indiquée dans cette commande. Par exemple, si vous entrez la valeur 20 et qu’une pièce jointe donnée ne peut être compressée à au moins 21%, MDaemon ne la compressera pas avant d’envoyer le message.



MDaemon doit d’abord compresser un fichier afin de déterminer à quel taux celui-ci doit être compressé. Par conséquent, cette fonctionnalité n’empêche pas les fichiers d’être compressés– elle évite simplement que les pièces jointes soient envoyées en format compressé lorsqu’elles ne peuvent pas être davantage compressées que la valeur indiquée. Autrement dit, si après avoir compressé le fichier, MDaemon ne peut le compresser plus que cette valeur, la compression sera ignorée et le message sera distribué avec ses pièces jointes en l’état.

Compresser si le total des pièces jointes est supérieur à X Ko
Lorsque la compression automatique de pièces jointes est activée, MDaemon tente de compresser les pièces jointes d’un message uniquement si leur total excède la valeur indiquée dans ce champ. Les messages dont la taille des pièces jointes est inférieure à ce seuil sont distribués normalement avec les pièces jointes en l’état.

Niveau de compression
Utilisez cette liste déroulante pour déterminer le degré de compression que MDaemon applique aux pièces jointes compressées. Vous pouvez choisir trois niveaux de compression : minimum (compression plus rapide mais moindre), moyen (valeur par défaut), ou maximum (compression moins rapide mais plus importante).

Utiliser un nom d’archive fixe
Activez cette option puis choisissez un nom si vous voulez que les pièces jointes compressées automatiquement aient un nom de fichier spécifique.

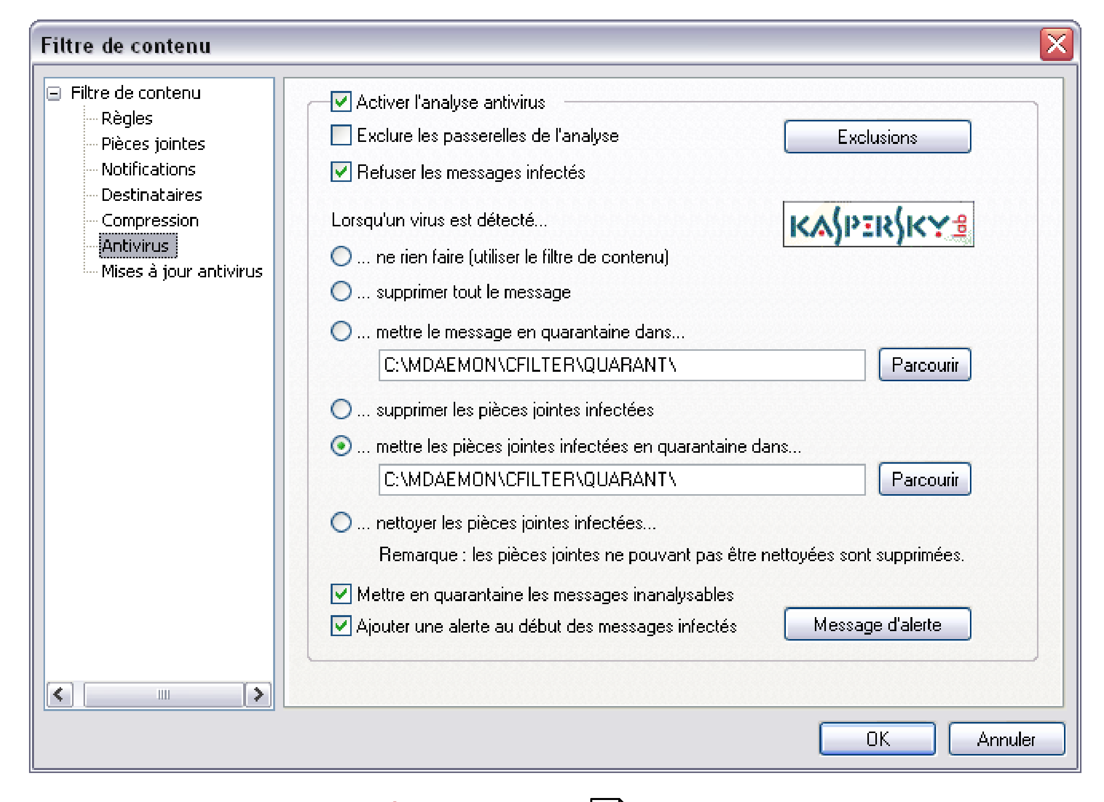
Exclusions

Fichiers exclus...
Cliquez sur ce bouton pour indiquer les fichiers que vous voulez exclure de la compression automatique. Lorsqu'une pièce jointe d'un message correspond à l'un de ces noms de fichiers, elle ne sera pas compressée, quels que soient les paramètres de compression. Les caractères jokers sont autorisés dans ces entrées. Par conséquent, vous pouvez par exemple indiquer "*.exe" pour que tous les fichiers se terminant par ".exe" ne soient pas compressés.

Domaines exclus...
Cliquez sur ce bouton pour indiquer les domaines des destinataires dont les messages seront exclus de la compression automatique. Les pièces jointes des messages liés à ces domaines ne seront pas compressées, quels que soient les paramètres de compression.

4.1.2 Antivirus

4.1.2.1 Antivirus



Cet onglet (et le suivant Mises à jour antivirus200) ne s'affichent que lorsque SecurityPlus for MDaemon est installé. SecurityPlus for MDaemon, est disponible à l'adresse www.altn.com.

Configuration

Activer l'analyse antivirus
Cochez cette case pour activer l'analyse antivirus de messages. Lorsque MDaemon reçoit un message avec des pièces jointes, il utilise SecurityPlus for MDaemon pour rechercher d'éventuels virus avant de distribuer le message à son destinataire.

Exclure les passerelles de l'analyse
Activez cette option si vous voulez que les messages liés à l'une des passerelles de domaine de MDaemon soient exclus de la détection de virus. Cela peut être utile aux utilisateurs qui souhaitent que la détection de virus de messages soit effectuée par le serveur de messagerie du domaine. POur en savoir plus, voir Passerelles de domaine406.

Refuser les messages infectés
Cochez cette option si vous souhaitez analyser les messages entrants au cours de la session SMTP (plutôt que d'attendre qu'elle soit terminée), et rejeter immédiatement les messages infectés. SecurityPlus for MDaemon n'accepte les messages et ne conclut la session qu'après avoir analysé chacun d'entre eux. Le serveur expéditeur en est donc toujours responsable car techniquement, les messages n'ont pas encore été remis. Les messages infectés sont rejetés avant même d'atteindre le serveur, ce qui permet d'éviter les procédures de quarantaine, de nettoyage et les messages de notification. En résumé, cela réduit considérablement le nombre de messages infectés et de notifications que vous et vos utilisateurs recevez.

Le résultat de l'analyse antivirus est consigné dans le fichier journal SMTP-(entrant). Plusieurs résultats sont possibles :

- Le message a été analysé et un virus a été découvert
- Le message a été analysé mais aucun virus n'a été découvert
- Le message n'a pas pu être analysé (impossible d'ouvrir certaines pièces jointes, comme celles au format ZIP)
- Le message n'a pas pu être analysé (car il dépasse la taille limite)
- Une erreur s'est produite au cours de l'analyse

Exclusions
Cliquez sur ce bouton pour indiquer les adresses des destinataires qui seront exclues de la détection de virus. SecurityPlus for MDaemon n'analysera pas les messages liés à ces adresses. Les caractères jokers sont autorisés dans ces adresses. Vous pouvez ainsi utiliser cette fonctionnalité pour exclure des domaines entiers ou des boîtes aux lettres spécifiques sur tous les domaines. Par exemple, "*@exemple.com" ou "VirusArchive@*".

Lorsqu'un virus est détecté...
Sélectionnez l'action à effectuer lorsque SecurityPlus for MDaemon détecte un virus.

...ne rien faire (utiliser le filtre de contenu)
Choisissez cette option si vous ne désirez effectuer aucune des actions ci-

dessous, et utiliser les règles du Filtre de contenu.

...supprimer tout le message
Lorsqu'un virus est détecté, cette option permet de supprimer entièrement le message, au lieu de ne supprimer que la pièce jointe. Ainsi, l'option Ajouter une alerte... ne s'applique pas. Toutefois, vous pouvez toujours envoyer un message de notification au destinataire à l'aide des options de l'onglet *Notifications*.

...mettre le message en quarantaine dans...
Cette option est identique à l'option *Supprimer tout le message* ci-dessus, mais le message est mis en quarantaine à l'emplacement indiqué au lieu d'être supprimé.

...supprimer les pièces jointes infectées
Cette option permet de supprimer les pièces jointes infectées. Le courrier concerné est distribué au destinataire sans la pièce jointe infectée. Vous pouvez utiliser l'option *Ajouter une alerte...* située en bas de cette boîte de dialogue pour ajouter un texte au message, afin d'informer l'utilisateur qu'une pièce jointe infectée a été supprimée.

...mettre les pièces jointes infectées en quarantaine dans...
Sélectionnez cette option et indiquez un emplacement dans le champ correspondant pour que les pièces jointes infectées soient mises en quarantaine dans ce fichier au lieu d'être supprimées ou nettoyées. Tout comme avec l'option *Supprimer* les pièces jointes infectées, le message est distribué au destinataire sans la pièce jointe.

...nettoyer les pièces jointes
Lorsque vous choisissez cette option, SecurityPlus for MDaemon tente de nettoyer la pièce jointe. Si elle ne peut pas être nettoyée, elle est supprimée.

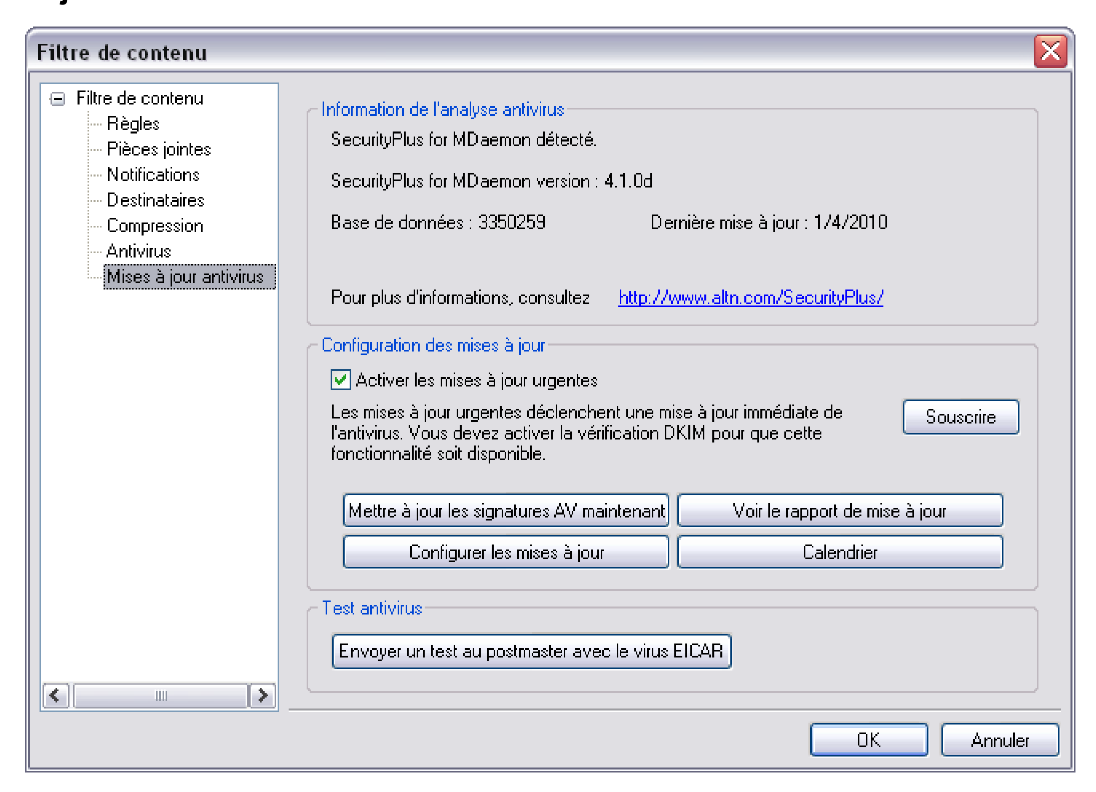
Ajouter une alerte au début des messages infectés
Cochez cette case pour qu'un texte d'avertissement soit ajouté en haut du message qui était infecté, avant qu'il ne soit distribué à son destinataire. Vous pouvez ainsi informer le destinataire des raisons de la suppression de la pièce jointe.

Message d'alerte
Cliquez sur ce bouton pour afficher un texte d'avertissement qui sera ajouté aux messages lorsque l'option *Ajouter une alerte...* est utilisée. Après avoir procédé aux modifications souhaitées dans ce texte, cliquez sur OK pour fermer cette boîte de dialogue et enregistrer les modifications.

Voir également :

Utilitaire de mise à jour antivirus 200
Filtre de contenu et SecurityPlus 177

4.1.2.2 Mises à jour antivirus



Utilisez les options de cet onglet pour mettre à jour manuellement ou automatiquement les définitions de virus de SecurityPlus for MDaemon. Vous disposez d'un programmateur pour les mises à jour automatiques, d'un rapport de mise à jour vous permettant de voir à quel moment et quelles mises à jour ont été téléchargées, ainsi que d'une fonction de test vous permettant de confirmer que la recherche de virus fonctionne correctement.

Informations de l'analyse antivirus

Cette section permet de voir si SecurityPlus for MDaemon est installé ainsi que la version utilisée. La date de votre dernière mise à jour de définition de virus est également indiquée.

Configuration des mises à jour

Activer les mises à jour urgentes
Cochez cette case pour activer la fonctionnalité de mises à jour urgentes. Lorsqu'elle est activée, SecurityPlus se connecte immédiatement à l'emplacement où se trouve la mise à jour urgente et la télécharge dès que MDaemon reçoit un message “Mise à jour urgente”. Pour recevoir ces messages, vous devez d'abord vous inscrire à la liste de diffusion "Mises à jour urgentes" (voir ci-dessous).

Souscrire
Ce bouton ouvre votre navigateur par défaut sur la page de Alt-N Technologies relative à l'abonnement aux mises à jour urgentes. Entrez le nom de votre domaine pour qu'il soit abonné à la liste de diffusion des mises à jour urgentes. Dès qu'une

mise à jour urgente des définitions de virus de SecurityPlus for MDaemon est disponible, un courrier est envoyé à ce domaine. Lorsque MDaemon reçoit ce message, SecurityPlus est immédiatement mis à jour.

Mettre à jour les signatures AV maintenant
Cliquez sur ce bouton pour mettre à jour les définitions de virus manuellement. L'outil de mise à jour se connecte alors immédiatement.

Configurer les mises à jour
Cliquez sur ce bouton pour configurer l'utilitaire de mise à jour202. Il contient quatre onglets : URL, Connexion, Proxy et Divers.

Voir le rapport de mise à jour
Cliquez sur ce bouton pour afficher le rapport de SecurityPlus for MDaemon. Il répertorie les heures, les actions effectuées et d'autres informations concernant toutes les mises à jour.

Calendrier
Cliquez sur ce bouton pour ouvrir le programmateur d'événements de MDaemon dans l'onglet Mises à jour antivirus147. Il contient également une option *Activer les mises à jour urgentes* identique à celle du même nom décrite ci-dessus.

Test antivirus

Envoyer un test au postmaster avec le virus EICAR
Cliquez sur ce bouton pour envoyer un message de test au postmaster, en incluant le fichier joint de virus EICAR. Cette pièce jointe est inoffensive ; elle sert à tester SecurityPlus for MDaemon. Dans l'onglet Filtre de contenu de l'interface principale, vous pouvez voir comment MDaemon agit avec le message lorsqu'il le reçoit. Par exemple, selon vos paramètres, vous aurez un extrait de l'enregistrement de type :

```
Mon 2008-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2008-02-25 18:14:49: > Message from: postmaster@mycompany.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@mycompany.com
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID: <MDAEMON10001200202251814.
AA1447619@mycompany.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1 (including
multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (sender)
```

```
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

Voir également :

Utilitaire de mise à jour antivirus 202
Antivirus 197
Filtre de contenu et SecurityPlus 177

4.1.2.2.1 Utilitaire de mise à jour antivirus

Cet utilitaire s'affiche en cliquant sur le bouton *Configurer les mises à jour* dans l'onglet Mises à jour antivirus 200 du Filtre de contenu.

Il contient quatre onglets :

URL

L'onglet URL contient une liste de sites auxquels SecurityPlus for MDaemon se connecte pour rechercher les mises à jour de signatures de virus. Vous pouvez laisser SecurityPlus gérer ces url automatiquement ou bien les saisir manuellement.

Choisir un point de départ au hasard dans la liste des URL
Si vous activez cette option les sites sont vérifiés de façon aléatoire plutôt que dans l'ordre dans lequel ils sont répertoriés.

Utiliser des signatures supplémentaires contre les virus et logiciels malveillants
Activez cette option si vous souhaitez également analyser les messages afin de vous protéger contre d'autres types de menaces :

- **Logiciels publicitaires (Adware)**—applications affichant des bannières publicitaires sur les ordinateurs des utilisateurs. Ils sont souvent inclus dans des logiciels proposés gratuitement.
- **Logiciels espions (Spyware)**—programmes surveillant l'utilisation d'un ordinateur. Ils peuvent par exemple obtenir son adresse IP, la version du système d'exploitation et du navigateur, la liste des sites les plus souvent consultés, les recherches effectuées... Ces informations sont ensuite utilisées pour des campagnes publicitaires (logiciels espions et publicitaires sont souvent liés).
- **Programmes proxy**—programmes utilisant un ordinateur à l'insu de son propriétaire pour recevoir et/ou transférer des fichiers ou des e-mails.
- **Porn-dialers**—programmes effectuant des connexions commutées surtaxées pour accéder à des ressources pornographiques. Le tarif de ces connexions

est considérablement élevé.

- Logiciels pouvant présenter des risques pour l'utilisateur (FTP, IRC, MIrc, RAdmin, utilitaires d'administration à distance)...
- **Page d'accueil**—certains logiciels malveillants modifient la page d'accueil d'Internet Explorer.

Connexion
L'onglet Connexion sert à indiquer le profil de connexion Internet que SecurityPlus for MDaemon doit utiliser lorsqu'il se connecte aux sites de mise à jour. L'option *Utiliser les options Internet du Panneau de configuration* utilise vos paramètres Internet par défaut. L'option *Configurer les paramètres Internet manuellement*, et les options qui suivent, peuvent être utilisées pour choisir manuellement un profil de connexion et indiquer le nom d'utilisateur et le mot de passe.

Proxy
Cet onglet contient des options permettant de configurer tous les paramètres de proxy HTTP ou FTP requis par votre configuration réseau pour la connexion aux sites de mise à jour.

Divers
Cet onglet contient les paramètres de journalisation de cet utilitaire.

Voir également :

Antivirus 197
Filtre de contenu et SecurityPlus 177

4.2 Protection instantanée

La protection instantanée est une technologie révolutionnaire de lutte contre les spams, les virus et les phishings capable de protéger l'infrastructure de MDaemon de façon proactive et automatique dès les premières minutes d'une attaque. Cette fonctionnalité est incluse dans SecurityPlus for MDaemon, et requiert au moins la version 3.0 de SecurityPlus for MDaemon et MDaemon Pro 9.5. Elle se trouve dans le menu Sécurité de MDaemon (Sécurité » Protection instantanée..., ou Ctrl+Shift+1).

La PI ne s'appuie en aucune façon sur le contenu des messages. Par conséquent, ce système ne requiert pas de règles heuristiques, ni de filtre de contenu ou de mises à jour de signatures. Ainsi, les techniques destinées à tromper les systèmes de protection (ajout de caractères, modifications orthographiques, différences de langue, ou de techniques de codage) n'ont aucun effet sur la détection des attaques. Ce système fonctionne grâce à une analyse mathématique de la structure des messages et des caractéristiques de distribution par SMTP. La PI analyse des "modèles" associés à l'envoi d'e-mails et les compare aux millions de messages collectés chaque jour dans le monde entier.

Les modèles provenant en temps réel du monde entier, la protection est efficace dès les premières minutes (et souvent les premières secondes) d'une nouvelle attaque. Une

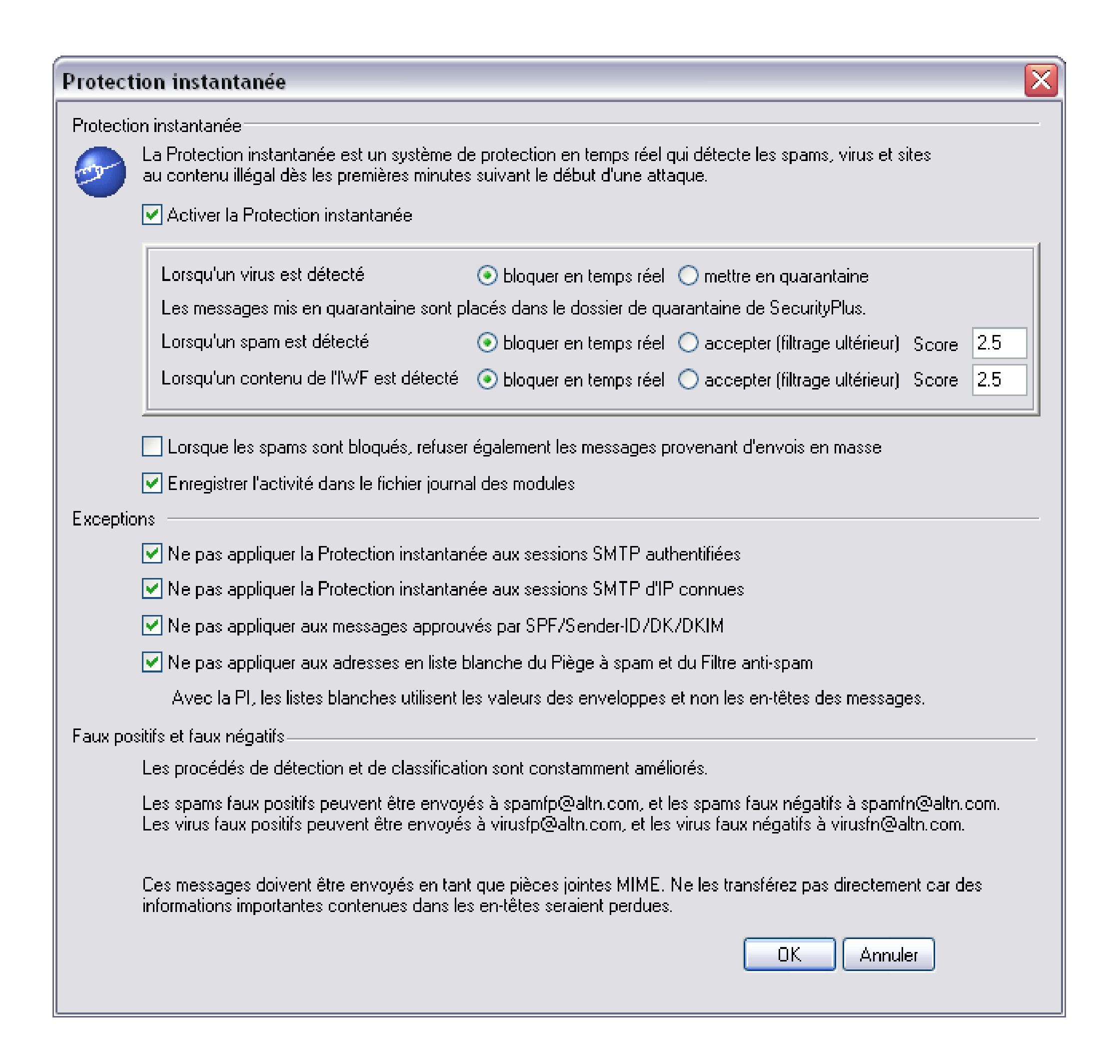
telle protection contre les virus est capitale. En effet, lors de l'apparition de nouveaux virus, les systèmes traditionnels nécessitent plusieurs heures pour créer et mettre en production les mises à jour des signatures. Durant cet intervalle, les utilisateurs n'étant pas protégés par SecurityPlus sont vulnérables. De même, les systèmes heuristiques traditionnels requièrent du temps pour analyser les spams et créer des règles de filtrage sécurisées.

Veuillez toutefois noter que la Protection instantanée de SecurityPlus ne remplace pas les solutions antivirus, anti-spam et anti-phishing traditionnelles. La PI constitue un niveau de sécurité supplémentaire venant s'ajouter aux outils d'analyse heuristique, d'analyse de contenu et basés sur des signatures également présents dans SecurityPlus et MDaemon. La PI est conçue pour détecter les nouvelles attaques déployées à grande échelle, plutôt que les spams et virus anciens ou spécifiques, facilement bloqués par les outils traditionnels.



La Protection instantanée est basée sur les technologies RPD et Zero-Hour de CommTouch. Elle extrait des "modèles" associés à l'envoi d'e-mails et les compare aux millions de messages collectés chaque jour dans le monde entier. Le contenu des messages n'est jamais transmis, et ne peut pas être déduit à partir des modèles.

Pour en savoir plus sur SecurityPlus et sur la Protection instantanée, voir le reste de cette section ou consulter : www.altn.com.



Protection instantanée

Activer la protection instantanée
Active la protection instantanée sur votre serveur. Les messages entrants sont analysés afin de détecter les nouvelles attaques de virus, spams, ou phishing. Les autres options permettent de déterminer les actions à effectuer et de configurer des exclusions.

Lorsqu'un virus est détecté...

...bloquer en temps réel
Lorsque la PI détecte un virus dans un message, celui-ci est rejeté au cours de la session SMTP. Dans ce cas, les messages ne sont pas mis en quarantaine, ni remis aux destinataires mais directement refusés par le serveur.

...mettre en quarantaine
Sélectionnez cette option si vous souhaitez mettre en quarantaine les virus détectés par la PI.

Lorsqu'un spam est détecté…

…bloquer en temps réel
une nouvelle attaque, le message est refusé. Il n'est pas marqué comme spam, ni distribué au destinataire, mais refusé par le serveur. Les messages simplement "suspects" sont acceptés mais le score de spam est modifié en fonction de l'option ci-dessous. Les messages provenant d'envois "en masse" ne sont pas bloqués par cette option, sauf si vous activez l'option *Lorsque les spams sont bloqués, refuser également les messages provenant d'envois en masse*. En effet ces messages peuvent faire partie de listes de diffusion ou lettres d'information adressées à un grand nombre de destinataires. Ainsi, il est généralement recommandé de ne pas refuser de type de messages.

…accepter (filtrage ultérieur)
Sélectionnez cette option si vous souhaitez que les spams soient acceptés par la PI. Ils seront alors soumis aux vérifications du Filtre anti-spam et du Filtre de contenu. De plus, leur score sera modifié en fonction de la valeur indiquée dans le champ *Score*.



Si vous utilisez l'option …accepter (filtrage ultérieur), le message n'est pas bloqué par la Protection instantanée, mais il risque d'être rejeté par le Filtre anti-spam 209 en fonction du score de spam obtenu.

Par exemple, si cette option ajoute 15 points au message, le message sera rejeté si le Filtre anti-spam est configuré rejeter les messages dont le score est supérieur à 15 points.

Score
Valeur ajoutée au score de spam lorsque l'option ci-dessus est activée et que la Protection instantanée détecte que le message fait partie d'une attaque.

Internet Watch Foundation (IWF)

Les options ci-dessous s'appliquent aux messages référant à des sites désignés comme pédophiles ou illégaux par l'IWF. La Protection instantanée utilise une liste d'URL fournie par l'IWF pour détecter ces messages. L'IWF est un organisme possédant une « hotline » indépendante destinée à repérer les sites dont le contenu est potentiellement illégal n'importe où dans le monde. Cet organisme travaille en association avec les services de police, les gouvernements, l'industrie du web et le public afin de lutter contre la diffusion des sites au contenu illégal. La liste des URL est mise à jour quotidiennement.

De nombreuses entreprises ont des règles internes concernant le contenu des messages envoyés et reçus par leurs employés, en particulier les éléments illégaux ou pornographiques. De plus, dans de nombreux pays l'envoi ou la réception de tels messages est interdit par la loi.

Plus d'informations sur l'IWF sont disponibles à l'adresse :

http://www.iwf.org.uk/

Lorsqu'un contenu de l'IWF est détecté...

...bloquer en temps réel
Choisissez cette option si vous souhaitez rejeter au cours de la session SMTP les messages liés à des sites signalés par l'IWF.

...accepter (filtrage ultérieur)
Sélectionnez cette option si vous souhaitez que les messages liés à des sites signalés par l'IWF soient acceptés par la PI. Ils seront alors soumis aux vérifications du Filtre anti-spam et du Filtre de contenu. De plus, leur score sera modifié en fonction de la valeur indiquée dans le champ *Score*.

Score
Valeur ajoutée au score de spam lorsque l'option ci-dessus est activée et que la Protection instantanée détecte que le message est lié à un site signalé par l'IWF.

Lorsque les spams sont bloqués, refuser également les messages provenant d'envois en masse
Certains messages légitimes comme les listes de diffusion ou les lettres d'information sont parfois envoyés à de très nombreux destinataires et considérés par la PI comme des envois "en masse" (bulk), par opposition aux spams "confirmés". Activez cette option si vous souhaitez que l'option *Lorsque qu'un spam/phishing est détecté...bloquer en temps réel* ci-dessus s'applique également à ce type de messages. Si cette option est désactivée, seuls les spams confirmés sont bloqués. Cette option peut s'avérer utile si vous recevez des lettres d'informations ou messages de liste de diffusion mais que vous ne pouvez pas mettre l'expéditeur en liste blanche.

Enregistrer l'activité dans le fichier journal des modules
Cochez cette case si vous souhaitez enregistrer l'activité de la PI dans le fichier journal des modules de MDaemon.

Exceptions

Ne pas appliquer la Protection instantanée aux sessions SMTP authentifiées
Lorsque cette option est activée, les messages envoyés au cours d'une session SMTP authentifiée ne sont pas soumis à la PI.

Ne pas appliquer la Protection instantanée aux sessions SMTP d'IP connues
Activez cette option si vous souhaitez que les messages provenant d'IP connues ne soient pas soumis à la Protection instantanée.

Ne pas appliquer aux messages approuvés par SPF/Sender-ID/DK/DKIM
Activez cette option si vous souhaitez que les messages considérés comme valides par SPF, Sender-ID, DK, ou DKIM et dont le domaine figure sur la liste des Domaines approuvés264 ne soient pas soumis à la Protection instantanée.

Ne pas appliquer aux entrées de la Liste des exceptions et de la Liste blanche (exp.) du Filtre anti-spam
La Liste des exceptions du Filtre anti-spam est basée sur le destinataire ou la valeur RCPT transmise lors de la session SMTP. La Liste blanche (exp.) est basée sur

l'expéditeur ou la valeur MAIL transmise lors de la session SMTP. Ces outils n'utilisent pas les en-têtes des messages.

Faux positifs et faux négatifs

Les faux positifs (messages légitimes considérés comme du spam) sont généralement très rares. Toutefois, si cela venait à se produire, vous pouvez envoyer ces messages à l'adresse **spamfp@altn.com** pour les spams ou **virusfp@altn.com** pour les virus. Cela permet d'améliorer les procédés de détection et de classification.

Les faux négatifs (spams considérés comme des messages positifs) se produisent plus souvent que les faux positifs. En effet, la PI n'est pas conçue pour bloquer tous les types de spams et de virus. Il s'agit d'une protection supplémentaire destinée à bloquer les nouvelles attaques lancées à grande échelle. Les messages anciens, ayant une cible spécifique, etc., peuvent être acceptés par la PI. Ils sont bloqués par les autres outils de sécurité de SecurityPlus et de MDaemon lors du traitement du message. Toutefois, vous pouvez envoyer les faux négatifs à **spamfn@altn.com** pour les spam/phishings ou **virusfn@altn.com** pour les virus.

Les messages doivent être envoyés en tant que pièces jointes MIME. Ne les transférez pas directement car des informations importantes pour la classification seraient perdues.

4.3 Filtre anti-spam

4.3.1 Filtre anti-spam

Le Filtre anti-spam inclut une technologie qui permet d'analyser de façon heuristique les messages électroniques entrants et de leur attribuer un "score" selon un système complexe de règles. Ce score est ensuite utilisé pour déterminer la probabilité pour qu'un message soit du spam et certaines actions peuvent être entreprises, en fonction de ce score : refuser le courrier, le marquer comme pouvant être du spam, etc.

Des adresses peuvent être inscrites sur liste blanche ou noire, ou être totalement dispensées de l'analyse du Filtre anti-spam. Il est possible d'insérer dans les messages un rapport sur le spam présentant leur score et la façon dont ces derniers ont été attribués. Vous pouvez aussi créer le rapport en tant que courrier séparé auquel le message indésirable d'origine sera attaché en pièce jointe. Si vous le souhaitez, vous pouvez utiliser le système d'apprentissage bayésien 212 afin que le Filtre anti-spam puisse apprendre, avec le temps, à identifier le spam de façon précise et devenir ainsi de plus en plus fiable.

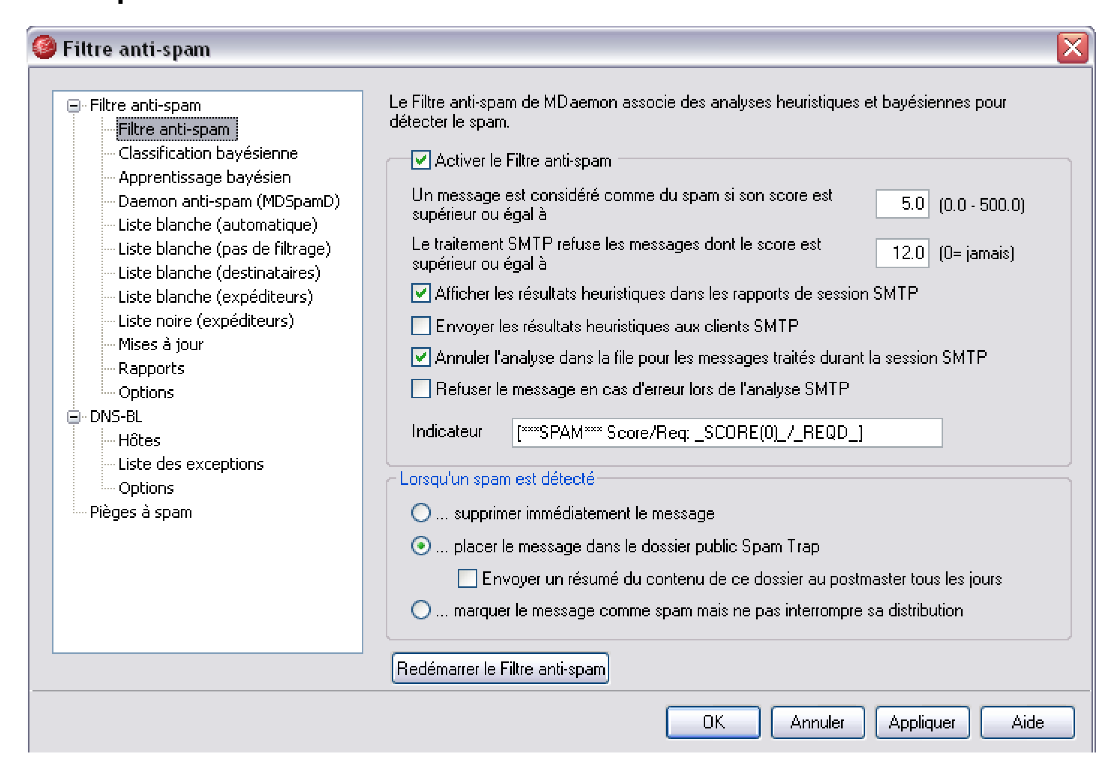
Enfin, grâce à l'analyse de plusieurs milliers de spams connus, les règles ont été optimisées au cours du temps : elles sont désormais extrêmement fiables quant à la détection des signes caractéristiques d'un message indésirable. Toutefois, en modifiant les fichiers de configuration du Filtre anti-spam, vous pouvez personnaliser ou ajouter des règles qui répondront à vos besoins particuliers. Le Filtre anti-spam de MDaemon utilise une technologie heuristique open-source reconnue appelée SpamAssassin :

`http://www.spamassassin.org`

Voir également :

[Filtre anti-spam](209)
[Listes noires DNS](231)

4.3.1.1 Filtre anti-spam



Activer le Filtre anti-spam

Cochez cette case pour activer le système d'attribution de scores aux messages du Filtre anti-spam. Aucune option du Filtre anti-spam ne sera disponible tant que vous n'aurez pas sélectionné cette option.

Un message est considéré comme du spam si son score est supérieur ou égal à X (0.0-500.0)

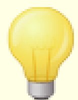
La valeur saisie dans cette case correspond au seuil minimal pour le spam que MDaemon compare au score de chaque message. Tous les messages qui obtiennent un score supérieur ou égal à cette valeur seront considérés comme du spam et les actions appropriées seront entreprises en fonction des paramètres que vous aurez configurés pour le Filtre anti-spam.

Le traitement SMTP refuse les messages dont le score est supérieur ou égal à X (0=jamais)

Utilisez cette option pour définir un score au-delà duquel le courrier considéré comme indésirable, sera rejeté. Lorsqu'un message obtient un score supérieur ou égal au seuil que vous avez fixé, il est alors rejeté en totalité au lieu d'être traité selon les autres fonctions et éventuellement distribué. La valeur de ce champ doit toujours être supérieure à celle saisie pour l'option ci-dessus *Un message est*

considéré comme du spam si son score … . Sinon, un message de ce type ne sera jamais considéré comme du spam et sera traité selon les autres options du Filtre anti-spam : il sera rejeté uniquement au moment de la distribution. Saisissez "0" dans ce champ si souhaitez que MDaemon ne rejette aucun message, quel que soit leur score.

Par exemple : si vous fixez le seuil pour le score des spams à 5.0 et le seuil de rejet à 10.0, tous les messages qui obtiennent un score de spam entre 5.0 (inclus) et 10.0 seront considérés comme du spam et traités en fonction des paramètres de la boîte de dialogue Filtre anti-spam. Quant aux messages qui obtiennent un score supérieur ou égal à 10.0, ils seront rejetés au cours du processus de distribution du courrier.



Vous devez surveiller la performance du Filtre anti-spam de temps à autre et ajuster les seuils des spams et de rejet pour qu'ils répondent à vos besoins. Toutefois, généralement un seuil pour les spams fixé à 5.0 bloquera la majorité des messages indésirables avec un taux de faux négatifs relativement faible, et très peu de faux positifs (le courrier marqué, à tort, comme spam). Un seuil de rejet fixé à 10 ou 15 entraînera uniquement le rejet de messages qui sont, presque systématiquement, indésirables. Il est très rare qu'un message légitime obtienne un score aussi élevé. Par défaut, le seuil de rejet est de 12.

Afficher les résultats heuristiques dans les rapports de session SMTP
Activez cette option pour enregistrer les résultats de l'analyse heuristique dans les journaux de session SMTP 98.

Envoyer les résultats heuristiques aux clients SMTP
Activez cette option pour afficher les résultats de l'analyse dans la session SMTP. Cette option n'est pas disponible si votre seuil de rejet est défini à "0" (voir "*Le traitement SMTP refuse les messages dont le score est supérieur ou égal à X*" ci-dessus).

Annuler l'analyse dans la file pour les messages traités durant la session SMTP
Par défaut, MDaemon analyse les messages pendant la session SMTP afin de déterminer s'ils doivent être refusés en fonction de leur score. Lorsqu'un message est accepté, MDaemon effectue une autre analyse dans la file d'attente afin d'appliquer les options du Filtre anti-spam. Lorsque cette option est activée, la deuxième analyse n'est pas effectuée. Cela peut réduire l'utilisation des ressources du processeur et améliorer l'efficacité du Filtre anti-spam. Cependant, dans ce cas seuls les en-têtes SpamAssassin par défaut sont ajoutés au message. Si vous avez modifié les en-têtes SpamAssassin par défaut ou indiqué des en-têtes personnalisés dans le fichier `local.cf`, ils seront ignorés.

Refuser le message en cas d'erreur lors de l'analyse SMTP
Activez cette option si vous souhaitez que le message soit refusé si une erreur se produit au cours de l'analyse effectuée pendant la session SMTP.

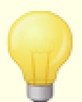
Indicateur
Cet indicateur sera inséré au début de l'en-tête Subject des messages dont le score est supérieur ou égal au seuil fixé. Vous pouvez le paramétrer pour qu'il contienne des informations concernant le score spam du message, et que ce dernier soit détecté et filtré en conséquence (à condition que le Filtre anti-spam soit configuré de façon à distribuer les messages). Cette méthode permet d'acheminer facilement les messages vers un dossier "spam" spécifique. Si vous souhaitez que l'insertion du score du message et de la valeur du seuil soient dynamiques, utilisez les indicateurs "_HITS_" pour le score et "_REQD _" pour le seuil requis. Vous pouvez également remplacer "_HITS_" par "_SCORE(0)_" car l'indicateur "_HITS_" ne reconnaît pas les scores commençant par zéro.

Exemple,

Si l'indicateur est : ***SPAM*** Score/Req: _HITS_/_REQD_ -
un score de 6.2 et le sujet : "Attention, ceci est un spam !"
il sera remplacé par "***SPAM*** Score/Req: 6.2/5.0 – Attention, ceci est un spam !"

Si "_SCORE(0)_" est remplacé par "_HITS_" on obtient "***SPAM*** Score/Req: 06.2/5.0 – Attention, ceci est un spam!"

Laissez le champ vide si vous ne souhaitez pas modifier le texte du sujet. Aucun indicateur ne sera inséré.



Cette option n'est pas disponible si vous avez choisi d'exécuter le daemon MDSpamD sur un autre poste (voir Daemon anti-spam 218).

Lorsqu'un spam est détecté...

Le Filtre anti-spam agit en fonction de l'option sélectionnée ci-dessous si un message indésirable obtient un score supérieur ou égal au seuil déterminé ci-dessus.

...supprimer immédiatement le message
Sélectionnez cette option si vous voulez tout simplement supprimer le courrier entrant dont le score dépasse la limite indiquée.

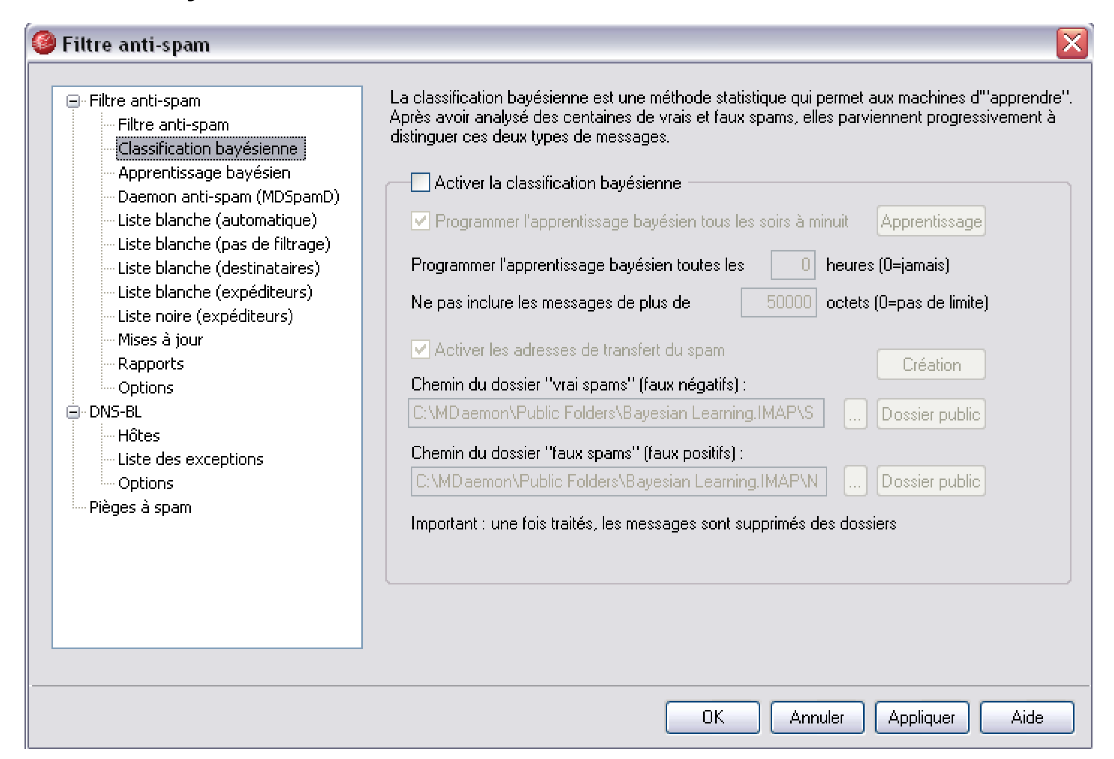
...placer le message dans le dossier public Piège à spam
Les messages ne sont pas distribués : ils sont marqués et déplacés dans le dossier public Piège à spam.

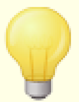
Envoyer un résumé du contenu du dossier au postmaster tous les jours
Si l'option précédente est activée, cochez cette case pour envoyer quotidiennement au postmaster un message contenant le résumé du contenu du dossier "Spam trap".

...marquer le message mais ne pas interrompre sa distribution
Sélectionnez cette option si vous souhaitez que les messages indésirables

continuent à être distribués à leurs destinataires respectifs mais qu'ils soient marqués comme spam à l'aide de différents en-têtes et/ou indicateurs définis ci-dessus et dans l'onglet Rapports 228. Cette option permet d'identifier les spams sans risquer de perdre les éventuels faux positifs.

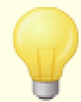
4.3.1.2 Classification bayésienne





Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un daemon antispam sur un autre serveur, car l'apprentissage bayésien s'effectue alors sur l'autre serveur (voir Daemon anti-spam) 218.

Le Filtre anti-spam supporte l'apprentissage bayésien, un processus statistique qui peut être utilisé pour analyser les spams et non spams. Il vise à optimiser avec le temps la fiabilité de la reconnaissance du courrier indésirable. Vous pouvez définir un dossier respectif pour les spams et les non spams qui seront analysés chaque soir à minuit. Tous les messages de ces dossiers seront référencés afin de les comparer statistiquement avec les nouveaux messages, et de déterminer la probabilité que ces derniers soient du spam. Le Filtre anti-spam peut ensuite augmenter ou diminuer le score d'un message en fonction des résultats de la comparaison effectuée grâce au système bayésien.



Le Filtre anti-spam n'appliquera pas la classification bayésienne aux nouveaux messages tant qu'une analyse bayésienne préalable n'a pas été effectuée sur le nombre minimum de

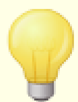
messages indiqué dans l'onglet Apprentissage bayésien 216. Ce délai est indispensable afin que le Filtre anti-spam possède suffisamment de données statistiques à analyser lors de la comparaison du système bayésien. Une fois que le système possède les messages requis, les références sont suffisantes pour pouvoir appliquer les résultats de la comparaison au score de chaque message entrant. Plus le nombre de messages analysés est important, plus la classification bayésienne devient précise.

Classification bayésienne

Appliquer la classification bayésienne
Activez cette option si vous souhaitez que le score des messages soit ajusté grâce à une comparaison avec les connaissances statistiques acquises.

Programmer l'apprentissage bayésien tous les soirs à minuit
Lorsque cette option est activée, le Filtre anti-spam analyse puis supprime tous les messages contenus dans les dossiers "Vrai spam" et "Faux spam" indiqués ci-dessous. Si vous souhaitez programmer l'apprentissage bayésien à un autre moment, décochez cette option et utilisez l'option *Programmer l'apprentissage bayésien toutes les X heures*. Pour que l'apprentissage ne s'effectue jamais de façon automatique, décochez cette option et indiquez "0" dans l'option ci-dessous.

Programmer l'apprentissage bayésien toutes les X heures (0=jamais)
Permet d'effectuer l'apprentissage bayésien à intervalles définis. Pour que l'apprentissage ne s'effectue jamais de façon automatique, indiquez "0" dans ce champ.



Si vous ne voulez pas que les messages soient supprimés après avoir été analysés, copiez le fichier `LEARN.BAT` dans `\MDaemon\App\`, renommez la copie `MYLEARN.BAT` et supprimez les deux lignes commençant par "`if exist`" vers la fin du fichier. Quand le fichier `MYLEARN.BAT` est présent dans ce dossier, MDaemon l'utilise à la place du fichier `LEARN.BAT`. Voir `SA-Learn.txt` dans `\MDaemon\SpamAssassin\` pour en savoir plus.

Pour en savoir plus sur la technologie de filtrage heuristique du spam et l'apprentissage bayésien, voir :

http://www.spamassassin.org/doc/sa-learn.html.

Ne pas inclure les messages de plus de X octets (0=pas de limite)
Indique la taille maximale des messages utilisés pour l'apprentissage.

Apprentissage
Cliquez sur ce bouton pour lancer manuellement une analyse bayésienne dans les

dossiers indiqués au lieu d'attendre l'analyse automatique.

Activer les adresses de transfert du spam
Transfère les spams et faux positifs à une adresse spécifique afin que le système bayésien puisse "apprendre" à les distinguer. Les adresses par défaut sont SpamLearn@<domaine.com> (spam) et HamLearn@<domaine.com> (faux positifs). Les messages envoyés à ces adresses doivent utiliser une session SMTP authentifiée avec SMTP AUTH. De plus, ils doivent être transférés en tant que pièce jointe de type message/rfc822. Les messages envoyés sous une autre forme ne seront pas pris en compte.

Pour changer ces adresses, modifiez le fichier `CFilter.INI` comme suit :

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

Remarque : le dernier caractère doit être "@".

Créer
Cliquez sur ce bouton pour créer automatiquement les dossiers publics IMAP 64 Spam et Non Spam utilisés par MDaemon.
Les dossiers créés sont les suivants :

`\Bayesian Learning.IMAP\`	Dossier racine
`\Bayesian Learning.IMAP\Spam.IMAP\`	Dossier utilisé pour les faux négatifs (spam n'étant pas marqué comme tel).
`\Bayesian Learning.IMAP\Non-Spam.IMAP\`	Dossier utilisé pour les faux positifs (messages légitimes considérés à tort comme du spam).

Par défaut, l'accès à ces dossiers n'est accordé qu'aux utilisateurs des domaines locaux et ils ne disposent que des droits "Consultation" et "Insertion". (Le postmaster possède les droits : "Consultation", "Lecture", "Insertion" et "Suppression").

Chemin du dossier "Vrais spams" (faux négatifs) :
Il s'agit du chemin d'accès au dossier qui sera utilisé pour l'analyse bayésienne des spams connus. Enregistrez dans ce dossier les messages que vous considérez comme du spam. Le processus d'enregistrement des messages dans ce dossier ne doit pas être automatisé car certaines erreurs pourraient se glisser : en effet, des non spams pourraient être analysés comme des spams, ce qui diminuerait la fiabilité des statistiques du Filtre bayésien.

Chemin du dossier "Faux spams" (faux positifs) :
Il s'agit du chemin d'accès au dossier qui sera utilisé pour l'analyse bayésienne des messages qui ne sont pas indésirables. Enregistrer dans ce dossier uniquement les messages que vous ne considérez pas comme de spam. Vous ne devez pas

automatiser le processus d'enregistrement des messages dans ce dossier car des erreurs pourraient se glisser : en effet, des spams pourraient être analysés comme des non spams, ce qui diminuerait la fiabilité des statistiques de l'apprentissage bayésien 216.

Dossier public
Cliquez sur l'un de ces deux boutons pour définir l'un de vos dossiers publics en tant que répertoire du Filtre bayésien. Ainsi, les utilisateurs peuvent facilement enregistrer leurs messages, qui ne sont pas correctement répertoriés comme spams ou non spams, dans votre répertoire bayésien pour qu'ils soient analysés. Notez toutefois que si un grand nombre de personnes ont accès à ces dossiers, la probabilité pour que certains messages soient enregistrés dans le mauvais répertoire est plus importante. Les statistiques peuvent donc être faussées et la fiabilité peut être réduite.

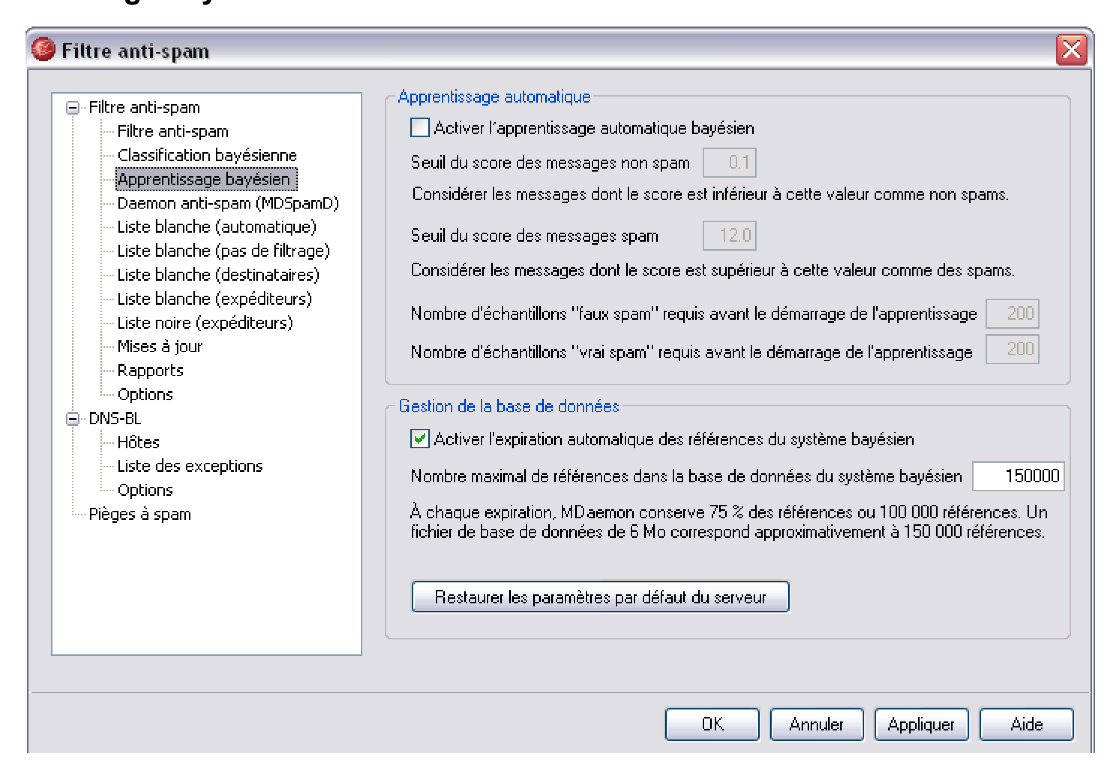


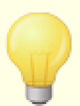
Si vous renommez un dossier public via un client de messagerie, Windows Explorer, ou d'une autre façon, vous devez modifier manuellement le chemin d'accès avec le nouveau nom de dossier. Si vous ne le faites pas, le Filtre anti-spam continuera à utiliser l'ancien chemin d'accès pour le dossier bayésien.

Voir également :

Apprentissage automatique 216
Pièges à spam 237

4.3.1.3 Apprentissage bayésien





Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un daemon antispam sur un autre serveur, car l'apprentissage bayésien s'effectue alors sur l'autre serveur (voir Daemon anti-spam) 218.

Apprentissage automatique

Activer l'apprentissage automatique bayésien
Avec l'apprentissage automatique bayésien, vous pouvez définir des seuils pour les scores des spams et des non spams. Tous les messages qui obtiennent un score inférieur au seuil des non spams seront traités comme des messages légitimes par le système d'apprentissage, et les messages qui obtiennent un score supérieur au score des spams seront traités comme des messages indésirables. Bien qu'en général l'apprentissage automatique ne soit pas recommandé, il peut être utile si vous fixez les valeurs des seuils avec précaution : les références expirées qui sont supprimées des fichiers de la base de données (voir *Activer l'expiration des références de la base de données du système bayésien* ci-dessous) peuvent être remplacées automatiquement.

Seuil du score des messages non spam
Les messages qui obtiennent un score inférieur à cette valeur seront traités comme des non spams par le système de classification bayésienne.

Seuil du score des messages spam
Les messages qui obtiennent un score supérieur à cette valeur seront traités comme

des spams par le système de classification bayésienne.

Nombre d'échantillons "faux spam" requis avant le démarrage de l'apprentissage
Nombre de messages faux positifs devant être soumis au filtre bayésien avant que l'analyse ne soit appliquée aux messages reçus. En effet, le Filtre anti-spam doit posséder suffisament d'éléments de comparaison pour effectuer une analyse correcte.

Nombre d'échantillons "vrai spam" requis avant le démarrage de l'apprentissage
Nombre de vrais spams devant être soumis au filtre bayésien avant que l'analyse ne soit appliquée aux messages reçus.

Gestion de la base de données

Activer l'expiration automatique des références du système bayésien
Sélectionnez cette option si vous voulez que le système bayésien supprime les références de la base de données lorsque le nombre maximal spécifié est atteint. Cette limite évite que votre base de données bayésienne soit de taille excessive.

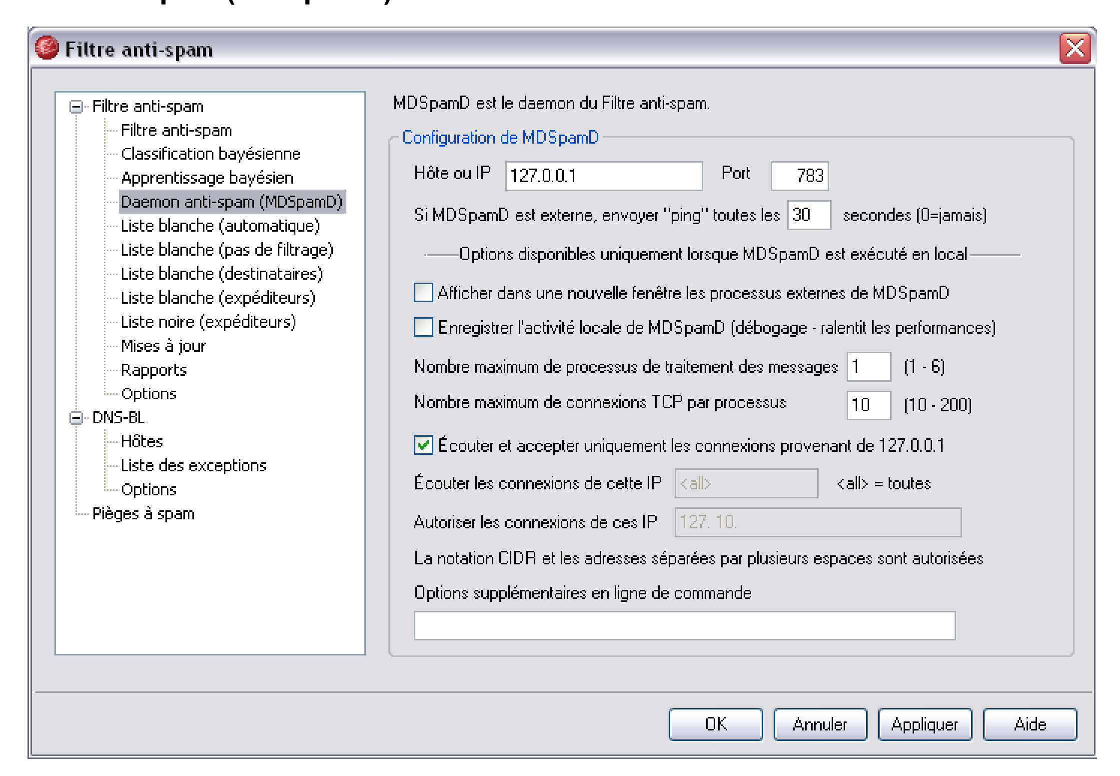
Nombre maximal de références dans la base de données du système bayésien
Il s'agit du nombre maximal de références pouvant être enregistrées dans la base de données bayésienne. Une fois cette valeur atteinte, le système bayésien supprime les anciennes références à hauteur de 75 %, soit 100 000 références au maximum. Le nombre de références ne descendra jamais au dessous de la plus grande de ces deux valeurs, peu importe le nombre de références expirées. Remarque : une base de données de 150 000 références fait environ 8 Mo.

Restaurer les paramètres par défaut du serveur
Cliquez sur ce bouton pour restaurer tous les paramètres par défaut des options avancées du système bayésien.

Voir également :

Classification bayésienne 212
Pièges à spam 237

4.3.1.4 Daemon anti-spam (MDSpamD)



Le système anti-spam s'exécute en tant que daemon distinct (MDSpamD) et les messages à analyser lui sont transmis automatiquement par TCP/IP. Cela augmente considérablement les performances du Filtre anti-spam et permet d'exécuter ce daemon en local, sur un autre serveur, ou bien d'utiliser un autre daemon SpamD situé sur un autre poste. Par défaut MDSpamD est exécuté en local et reçoit les messages sur le port 783 à l'adresse 127.0.0.1., mais vous pouvez configurer un daemon différent à un autre emplacement.

Hôte ou IP
Les messages à analyser sont transmis à l'hôte ou adresse IP indiqué(e) dans ce champ. Utilisez 127.0.0.1 pour exécuter MDSpamD en local.

Port
Numéro de port sur lequel les messages sont envoyés (par défaut : 783).

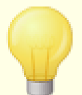
Si MDSpamD est externe, envoyer "ping" toutes les X secondes
Si vous utilisez MDSpamD ou un autre SpamD sur un serveur différent de MDaemon, cette option permet d'envoyer la commande « ping » à intervalles réguliers afin de vérifier la connexion entre les deux postes. Indiquez « 0 » si vous ne souhaitez pas envoyer cette commande.

Options disponibles uniquement lorsque MDSpamD est exécuté en local

Afficher dans une nouvelle fenêtre les processus externes de MDSpamD
Lorsque MDSpamD est exécuté en local, activez cette option si vous souhaitez qu'il soit exécuté dans un processus externe. Ainsi, les informations concernant

MDSpamD sont affichées dans cette fenêtre et non dans l'interface ou les journaux de MDaemon. Cela peut améliorer les performances. Cependant, lorsque cette option est activée, aucun fichier journal n'est créé et les données de MDSpamD ne sont pas consignées dans l'onglet *Sécurité »MDSpamD* de l'interface principale de MDaemon.

Enregistrer l'activité locale de MDSpamD (débogage—ralentit les performances)
Cochez cette option si vous souhaitez enregistrer toutes les activités locales de MDSpamD. Cette option ne peut pas être associée à l'option ci-dessus. De plus, si vous utilisez les identifiants de connexion de l'onglet Service Windows170 au lieu d'exécuter MDaemon avec le compte système, l'activité de MDSpamD n'est pas enregistrée.



L'utilisation de cette option peut diminuer les performances de votre système de messagerie. Il est recommandé de ne l'utiliser qu'à des fins de débogage.

Nombre maximum de processus de traitement des messages (1-6)
Nombre maximum de thread utilisés par MDaemon.

Nombre maximum de connexions TCP par processus (10-200)
Nombre maximum de connexions TCP acceptées par un thread MDSpamD avant d'en ouvrir un autre.

Écouter et accepter uniquement les connexions provenant de 127.0.0.1
Cochez cette option pour que MDSpamD refuse toute connexion extérieure.

Écouter les connexions de cette IP
Si l'option précédente est désactivée, vous pouvez limiter les connexions à une adresse spécifique. Indiquez <all> pour accepter toutes les adresses.

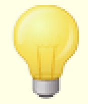
Autoriser les connexions de ces IP
Indiquez les adresses pour lesquelles MDSpamD doit accepter les connexions entrantes. Les connexions provenant d'IP ne figurant pas dans ce champ seront rejetées. Cela permet de partager le traitement du spam avec un autre serveur.

Options supplémentaires en ligne de commande

MDSpamD accepte de nombreuses options en ligne de commande, dont la liste complète est disponible à l'adresse :

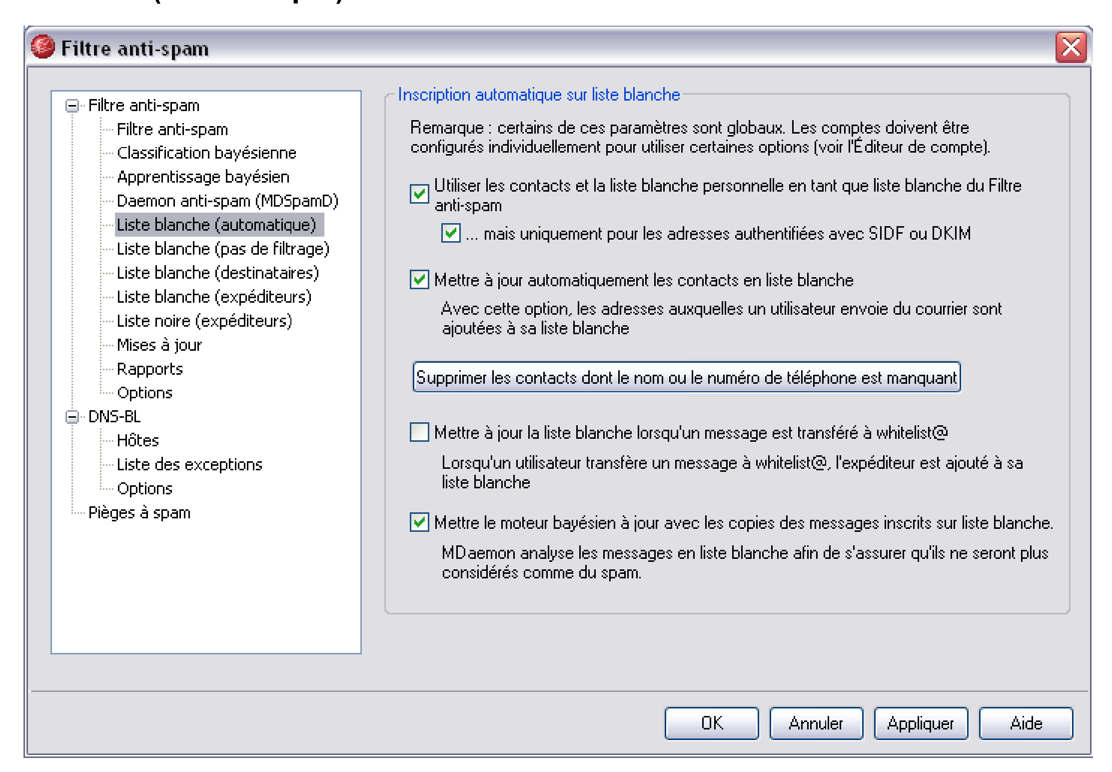
http://spamassassin.apache.org/

Pour utiliser une de ces options, construisez une chaîne contenant la commande souhaitée puis saisissez-la ici.



Certaines de ces options sont disponibles dans cette boîte de dialogue. Il n'est donc pas nécessaire de les modifier manuellement avec une ligne de commande.

4.3.1.5 Liste blanche (automatique)



Inscription automatique sur liste blanche

Utiliser les contacts et la liste blanche personnelle en tant que liste blanche du Filtre anti-spam

Cette option permet d'utiliser le carnet d'adresses par défaut et la liste blanche personnelle de chaque utilisateur en tant que liste blanche du Filtre anti-spam. Lorsque MDaemon reçoit un message, il vérifie si l'expéditeur se trouve dans la liste blanche ou dans le carnet d'adresses par défaut d'un utilisateur local. Si l'expéditeur se trouve dans l'un de ces emplacements, le message est automatiquement mis en liste blanche. Si vous ne souhaitez pas que cette option s'applique à tous les utilisateurs MDaemon, vous pouvez la désactiver pour certains d'entre eux en décochant la case *Utiliser les contacts en liste blanche et du carnet d'adresses par défaut en tant que liste blanche du Filtre anti-spam* dans l'onglet Options 328 de l'Éditeur de comptes.

Avec ComAgent, vous pouvez très facilement mettre à jour et synchroniser votre carnet d'adresses avec WorldClient, Outlook, Outlook Express, le carnet d'adresses Windows, et d'autres clients de messagerie MAPI qui utilisent le carnet d'adresses Windows.

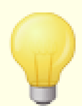
...mais uniquement pour les adresses vérifiées avec SIDF ou DKIM

Lorsque cette option est activée, MDaemon ajoute à la liste blanche uniquement les adresses authentifiées avec Sender ID Framework 249 (SIDF) ou DomainKeys

Identified Mail 251 (DKIM).

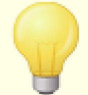
Mettre à jour automatiquement les contacts en liste blanche
Cette option ajoute automatiquement à la liste blanche personnelle de l'utilisateur toutes les adresses non locales auxquelles il envoie du courrier. Si vous utilisez cette option en association avec la précédente, le nombre de faux positifs devrait être considérablement réduit.

Si vous ne souhaitez pas activer la mise à jour automatique pour certains utilisateurs seulement, il est possible de la désactiver en décochant *Ajouter les destinataires des messages aux contacts en liste blanche* dans l'onglet Options 328 de l'Éditeur de comptes.



Cette option est désactivée pour les comptes utilisant l'autorépondeur.

Supprimer les contacts dont le nom ou le numéro de téléphone est manquant
Cliquez sur ce bouton si vous souhaitez supprimer du carnet d'adresses par défaut de tous les utilisateurs tous les contacts contenant uniquement une adresse e-mail. Si un contact n'a pas au moins un nom ou un numéro de téléphone il sera supprimé. Cette option est destinée à nettoyer les contacts ajoutés par l'option de liste blanche automatique des versions précédentes de MDaemon. En effet, dans les versions précédentes les adresses étaient ajoutées au carnet d'adresses par défaut au lieu de la liste blanche personnelle. Par conséquent les carnets d'adresses contenaient parfois des contacts que les utilisateurs ne souhaitaient pas ajouter.



N'utilisez cette option qu'avec précaution, car des contacts contenant uniquement une adresse e-mail peuvent être légitimes.

Mettre à jour la liste blanche lorsqu'un message est transféré à whitelist@
Lorsque cette option est activée, les utilisateurs peuvent ajouter automatiquement l'expéditeur d'un message à leur liste blanche en transférant ce message à `whitelist@<domain.com>` (à condition que l'option *Utiliser les contacts en liste blanche et du carnet d'adresses par défaut en tant que liste blanche du Filtre anti-spam* soit activée dans l'onglet Options de l'Éditeur de comptes). L'adresse sur liste blanche est récupérée dans le champ « From » des messages transférés.

Les messages transférés vers whitelist@<domain.com> doivent être sous forme de pièces jointes du type message/rfc822, et provenir d'une session SMTP authentifiée par SMTP AUTH. Les messages qui ne répondent pas à ces critères ne seront pas traités.

Il est possible de changer l'adresse utilisée par MDaemon, en modifiant le fichier `CFILTER.INI` comme suit :

```
[SpamFilter]
WhiteListAddress=monadresse@
```

Remarque : le dernier caractère doit être "@".

Mettre le moteur bayésien à jour avec les copies des messages inscrits sur liste blanche
Les messages de la liste blanche sont copiés dans le dossier d'apprentissage bayésien "Faux spams" (défini dans l'onglet Filtre bayésien). Cela permet de fournir des échantillons de "Faux spam" au moteur bayésien de façon automatique. Plus le nombre d'échantillons est élevé, plus le moteur est efficace, ce qui réduit considérablement les faux positifs (messages considérés par erreur comme du spam).

Cette fonctionnalité ne s'applique qu'aux messages entrants adressés à un utilisateur local et dont l'expéditeur figure dans son carnet d'adresses WorldClient. S'il s'agit d'un message sortant, c'est le destinataire qui doit figurer dans le carnet d'adresses. Si vous souhaitez que cette fonctionnalité ne s'applique pas aux messages sortants, modifiez le fichier `MDaemon.ini` comme suit :

```
[SpamFilter]
UpdateHamFolderOutbound=No (par défaut = Yes)
```

Lorsque cette fonctionnalité s'applique à un message, ce dernier est copié dans le dossier d'apprentissage bayésien "Faux spam", même si l'apprentissage bayésien est désactivé. Ainsi des échantillons de "faux spam" sont prêts à être analysés dès son activation. Cependant, tous les messages concernés ne sont pas copiés dans le dossier d'apprentissage : MDaemon arrête lorsqu'une certaine quantité est atteinte, et ne copie ensuite qu'un message à intervalles réguliers. Par défaut, les vingt-cinq premiers messages concernés sont copiés, puis un message sur dix. Le nombre initial correspond à celui désigné dans l'option d'apprentissage bayésien218 *Nombre d'échantillons "faux spam" requis avant le démarrage de l'apprentissage*. Si vous souhaitez changer l'intervalle de copie des messages suivants, modifiez le fichier MDaemon.ini comme suit :

```
[SpamFilter]
HamSkipCount=10 (par défaut = 10)
```

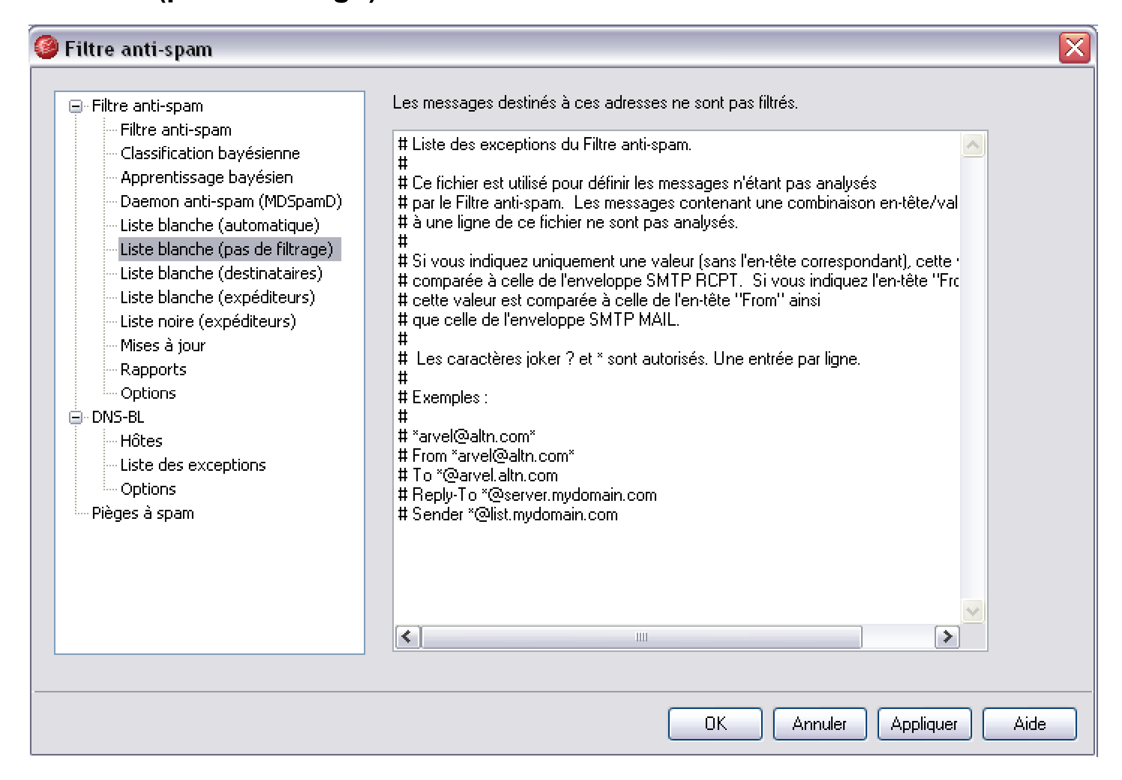
Enfin, au bout d'un certain nombre d'échantillons, l'apprentissage recommence du début : vingt-cinq messages copiés, puis un sur dix (ou une autre valeur si vous avez modifié ce paramètre). Par défaut, l'apprentissage recommence lorsque 500 messages ont été copiés. Si vous souhaitez changer cette valeur, modifiez le fichier MDaemon.ini comme suit :

```
[SpamFilter]
HamMaxCount=500 (par défaut = 500)
```

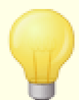


Cette option n'est pas disponible si MDaemon est configuré pour utiliser un daemon antispam sur un autre serveur, car l'apprentissage bayésien s'effectue alors sur l'autre serveur (voir Daemon anti-spam)218.

4.3.1.6 Liste blanche (pas de filtrage)

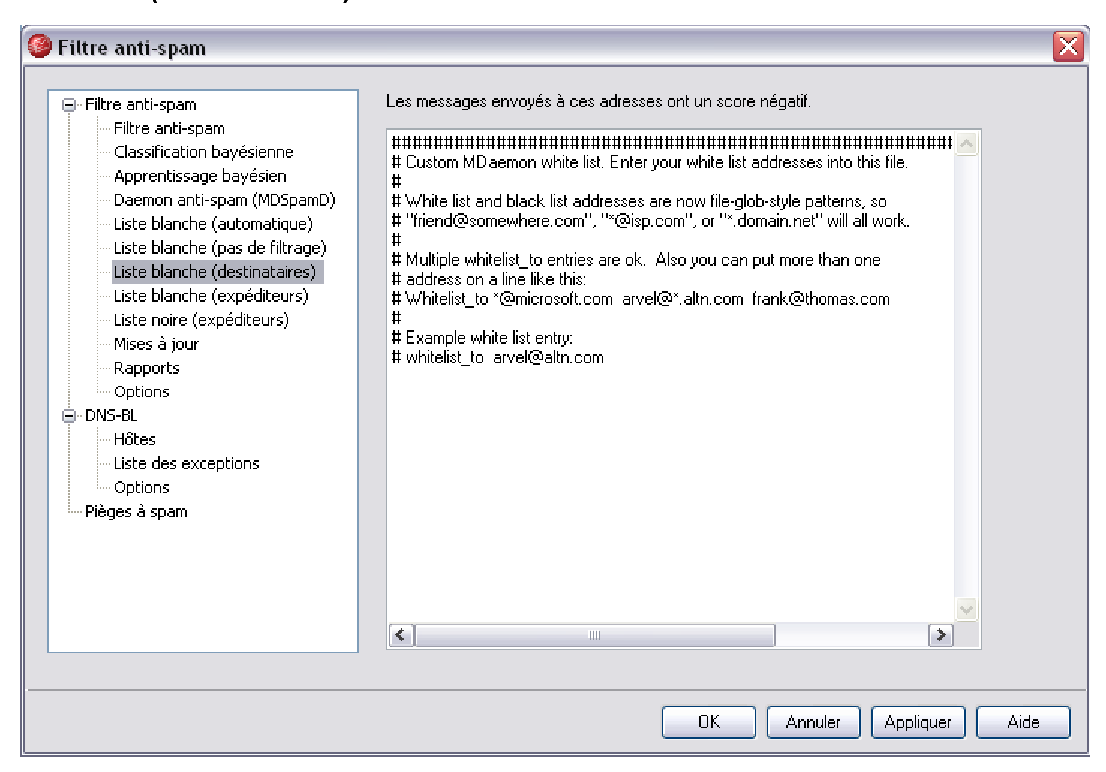


Les messages destinés à ces adresses ne sont pas filtrés
Indiquez les adresses des destinataires pour lesquels vous souhaitez pas effectuer d'analyse anti-spam sur les messages reçus.

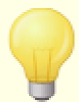


Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un autre SpamD sur un autre serveur car la liste sera conservée sur ce serveur (voir Daemon anti-spam 218).

4.3.1.7 Liste blanche (destinataires)

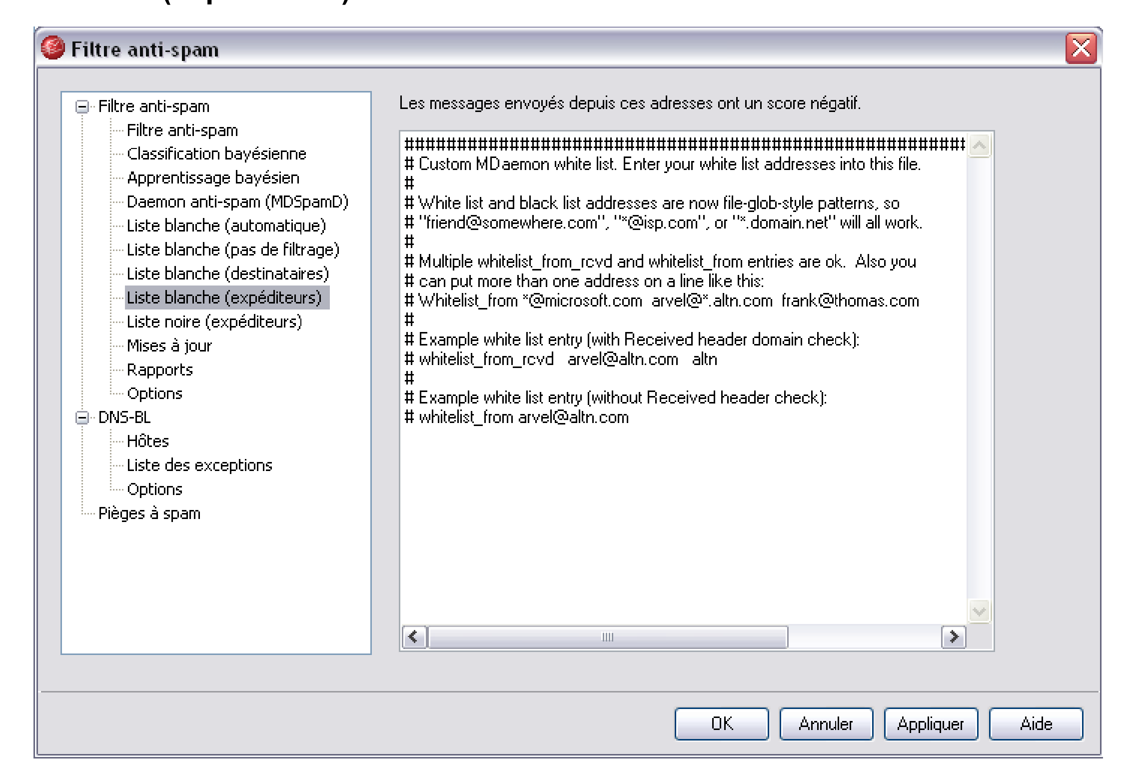


Les messages envoyés à ces adresses ont un score négatif
Il est possible qu'un message envoyé à une adresse inscrite sur cette liste blanche soit considéré comme du spam. Pour éviter cette confusion, la valeur indiquée dans l'onglet Filtre anti-spam sera enlevée au score des messages envoyés aux adresses inscrites sur cette liste blanche.

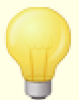


Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un autre SpamD sur un autre serveur car la liste sera conservée sur ce serveur (voir Daemon anti-spam 218).

4.3.1.8 Liste blanche (expéditeurs)

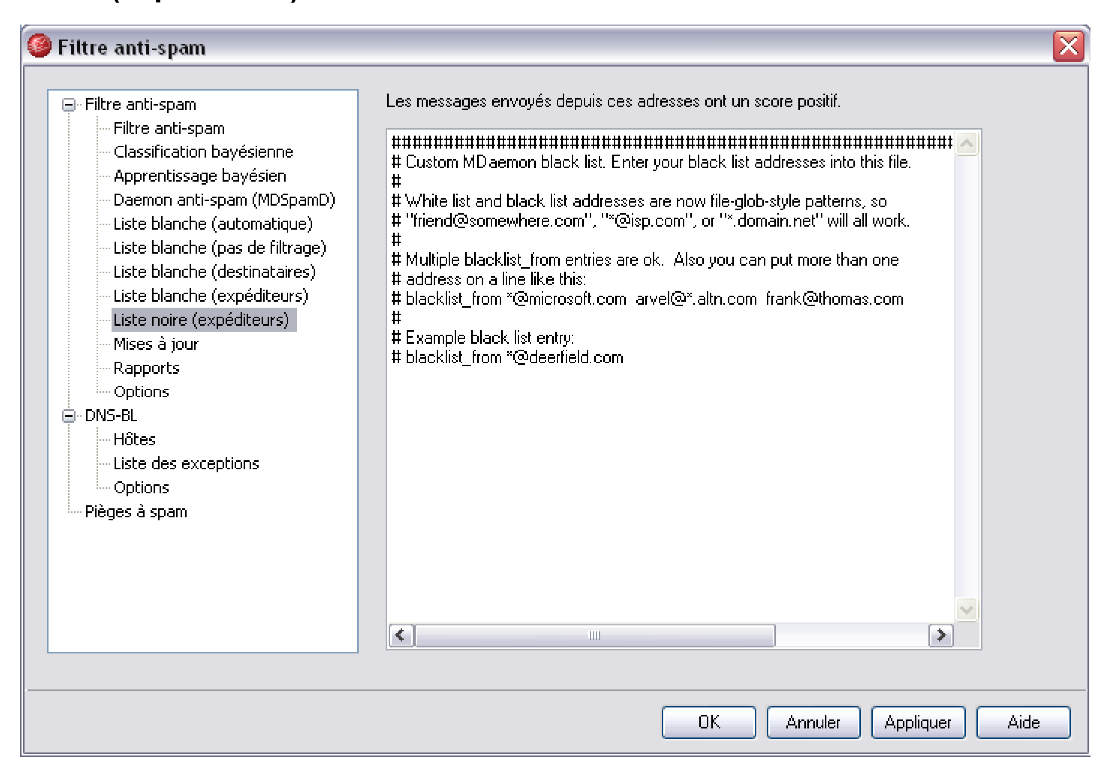


Les messages envoyés depuis ces adresses ont un score négatif
Il est possible qu'un message envoyé par une adresse inscrite sur cette liste blanche soit considéré comme du spam. Pour éviter cette confusion, la valeur indiquée dans l'onglet Filtre anti-spam sera enlevée au score des messages envoyés par les adresses inscrites sur cette liste blanche.

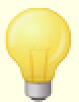


Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un autre SpamD sur un autre serveur car la liste sera conservée sur ce serveur (voir Daemon anti-spam 218).

4.3.1.9 Liste noire (expéditeurs)

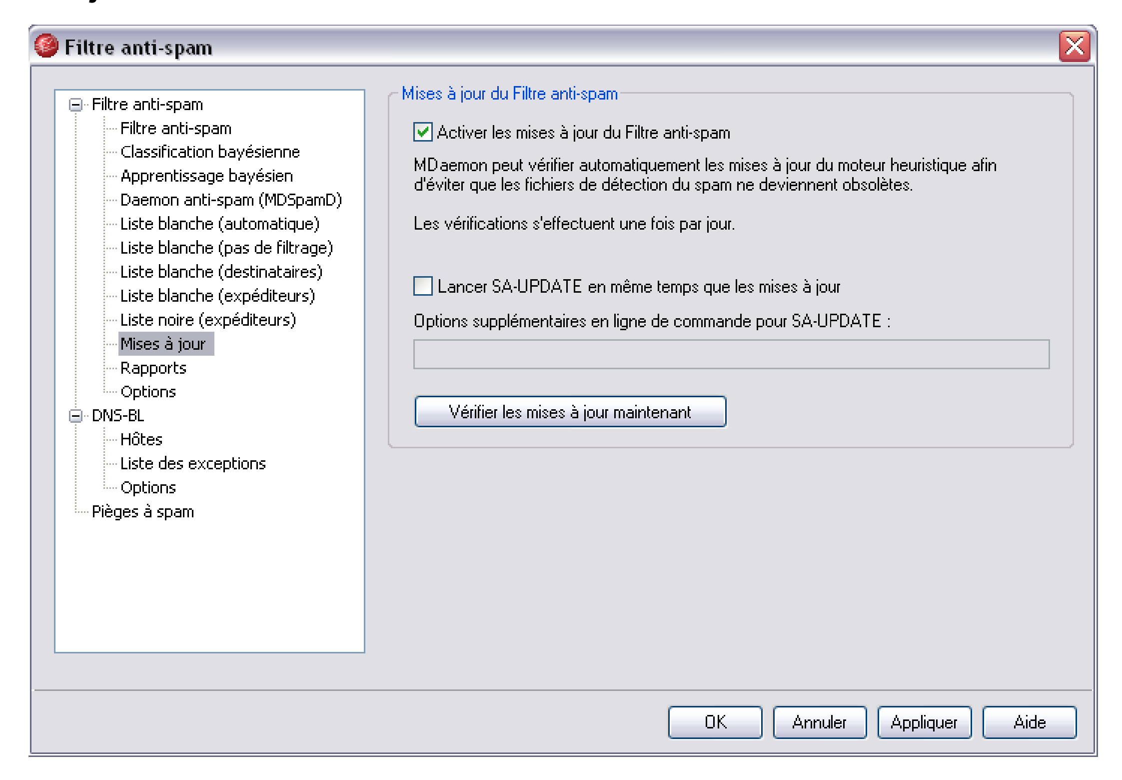


Les messages envoyés depuis ces adresses ont un score positif
Il est possible qu'un message envoyé à une adresse inscrite sur cette liste noire ne soit pas considéré comme du spam. Pour éviter ce problème, la valeur indiquée dans l'onglet Filtre anti-spam sera ajoutée au score des messages provenant des adresses inscrites sur cette liste noire.



Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un autre SpamD sur un autre serveur car la liste sera conservée sur ce serveur (voir Daemon anti-spam 218).

4.3.1.10 Mises à jour



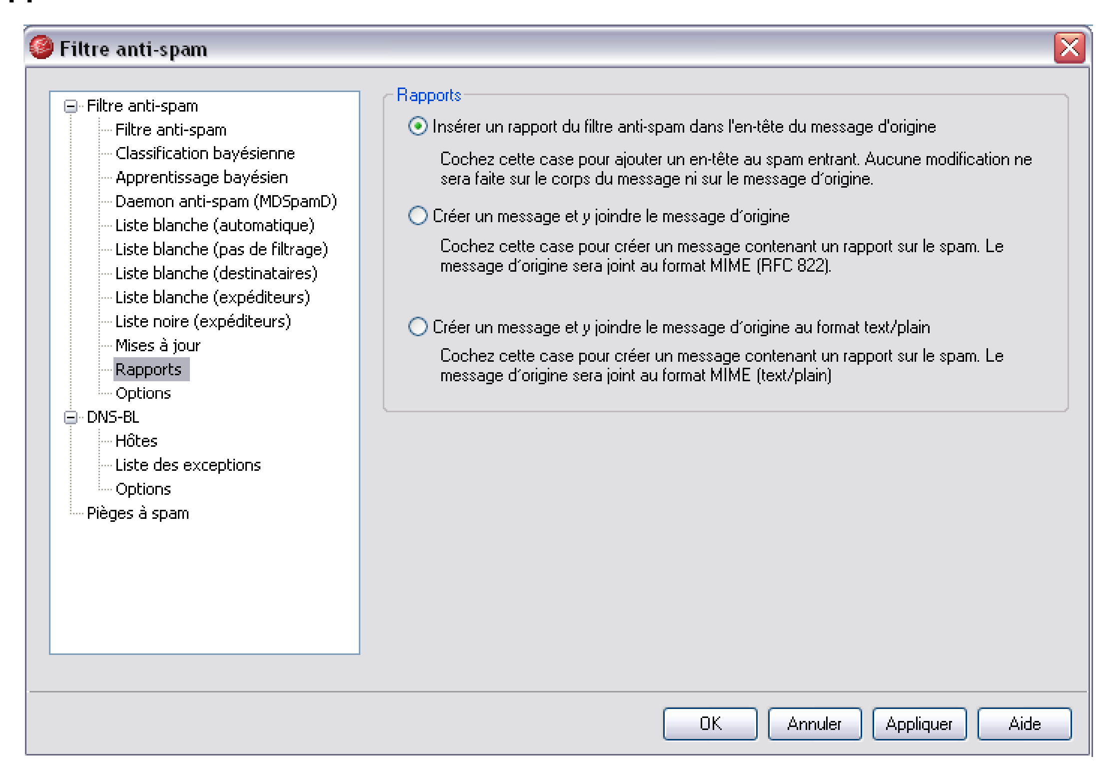
Mises à jour du Filtre anti-spam

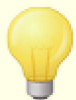
Activer les mises à jour du Filtre anti-spam
Cochez cette case si vous souhaitez que MDaemon recherche quotidiennement les mises à jour du moteur heuristique.

Lancer SA-UPDATE en même temps que les mises à jour
Cochez cette case si vous souhaitez récupérer les mises à jour depuis `updates.spamassassin.org` en plus des mises à jour de Alt-N Technologies. Cela permet de s'assurer que les règles de SpamAssassin sont toujours à jour.

Vérifier les mises à jour maintenant
Cliquez sur ce bouton pour vérifier manuellement les mises à jour.

4.3.1.11 Rapports





Cet onglet n'est pas disponible si MDaemon est configuré pour utiliser un daemon antispam sur un autre serveur (voir Daemon anti-spam 218).

Rapports

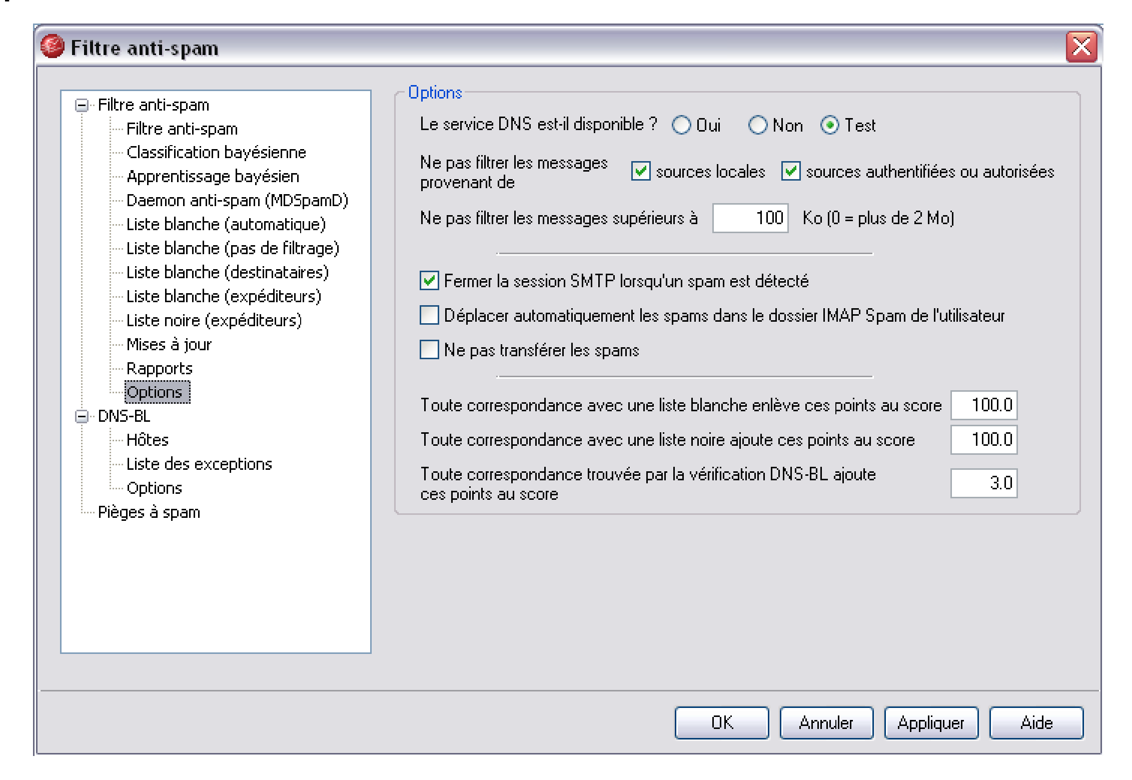
Insérer un rapport du filtre anti-spam dans l'en-tête du message d'origine
Option par défaut. Sélectionnez cette option si vous souhaitez que le Filtre anti-spam insère un rapport sur le spam dans les en-têtes de tous les messages indésirables. Voici un exemple de rapport :

```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
  *  3.0 -- Message has been marked by MDaemon's DNS-BL
  *  2.9 -- BODY: Impotence cure
  *  2.2 -- BODY: Talks about exercise with an exclamation!
  *  0.5 -- BODY: Message is 80% to 90% HTML
  *  0.1 -- BODY: HTML included in message
  *  1.6 -- BODY: HTML message is a saved web page
  *  2.0 -- Date: is 96 hours or more before Received: date
---- End of Spam Filter results
```

Créer un message et y joindre le message d'origine
Sélectionnez cette option si vous voulez que la réception d'un message indésirable entraîne la création d'un message contenant le rapport sur le spam. Le spam d'origine sera attaché à ce message en pièce jointe.

Créer un message et y joindre le message d'origine au format texte/plain
Semblable à l'option concernant les rapports sur le spam, celle-ci entraîne la création d'un message contenant le rapport sur le spam, auquel le message d'origine est attaché en pièce jointe. La différence réside dans le fait que le message d'origine sera joint au format text/plain. Dans la mesure où le spam contient parfois du code HTML, unique pour chaque message, et qu'il peut fournir au spammeur l'e-mail et l'adresse IP utilisés pour l'ouvrir, cette méthode permet de convertir le code HTML en texte clair, et d'éviter tout problème.

4.3.1.12 Options



Le service DNS est-il disponible ?
Indiquez si les serveurs DNS sont disponibles pour le Filtre anti-spam.

Oui - les DNS sont disponibles. Les règles de type SURBL/RBL pourront donc être utilisées.

No - les DNS ne sont pas disponibles. Les règles nécessitant les DNS ne pourront pas être utilisées.

Test - MDaemon vérifie la disponibilité des DNS et les utilise s'ils sont présents

(paramètre par défaut).

Ne pas filtrer les messages provenant de...

sources locales
Cochez cette case pour que les messages envoyés par des utilisateurs et domaines locaux soient dispensés du contrôle du Filtre anti-spam.

sources authentifiées ou autorisées
Activez cette option si vous souhaitez que les messages envoyés par des domaines autorisés ou des expéditeurs authentifiés soient dispensés du contrôle du Filtre anti-spam.

Ne pas filtrer les messages supérieurs à X Ko (0 = filtrer tous les messages)
En général, les messages indésirables sont de petite taille car les spammeurs veulent distribuer un maximum de messages le plus rapidement possible. Si vous souhaitez que les messages dépassant une certaine taille soient dispensés du contrôle du filtre, entrez cette valeur (en Ko) dans le champ correspondant. Saisissez "0" si vous souhaitez que tous les messages soient filtrés, quelle que soit leur taille.

Fermer la session SMTP lorsqu'un spam est détecté
Cette option est activée par défaut et ferme la session SMTP si l'analyse en ligne détecte un spam.

Déplacer automatiquement les spams dans le dossier IMAP Spam de l'utilisateur
Sélectionnez cette option pour que MDaemon enregistre automatiquement les messages indésirables détectés par le Filtre anti-spam dans le dossier "Spam" de chaque utilisateur (si un dossier de ce nom existe). De même, il créera automatiquement ce dossier IMAP pour chaque nouveau compte utilisateur.

Lorsque que vous cochez cette case, une boîte de dialogue s'ouvre et vous demande si vous voulez que MDaemon crée ce dossier pour les comptes utilisateurs existants. En cliquant sur "Oui", un dossier sera créé pour tous les utilisateurs, alors que si vous cliquez sur "Non", ce dossier sera créé uniquement à chaque ajout d'un utilisateur. Les dossiers existants pour un ou l'ensemble des utilisateurs ne seront en aucun cas modifiés.

Ne pas transférer les spams
Activez cette option si vous ne voulez pas que les messages indésirables soient transférés.



Les options suivantes ne sont pas disponibles si vous avez choisi d'exécuter le daemon MDSpamD sur un autre poste. Voir Daemon anti-spam 218 pour en savoir plus.

Toute correspondance avec une liste blanche enlève ces points au score
Même si vous inscrivez une adresse dans les onglets Liste blanche (dest) 224 ou Liste blanche (exp) 225 du Filtre anti-spam, il est possible qu'un message provenant ou à

destination de cette adresse soit tout de même considéré comme du spam. La valeur inscrite dans ce champ sera simplement enlevée du score de chacune des adresses inscrites sur liste blanche. Imaginons, par exemple, que le seuil du score pour les spams est 5.0 et que la valeur dans le champ de cette option est 100. Si un message entrant, particulièrement indésirable, obtient le score 105.0, ou plus, avant le retrait du score de liste blanche, le score final de ce message sera 5.0 au moins, ce qui l'identifie comme un spam.



Si vous souhaitez que les messages adressés à certains destinataires ne soient pas du tout vérifiés par le Filtre anti-spam, indiquez leur adresse dans la Liste blanche (pas de filtrage) 223. Il est également possible d'éviter l'analyse du Filtre anti-spam à l'aide des options de Liste blanche (automatique) 220.

Toute correspondance avec une liste noire ajoute ces points au score
Cette valeur est ajoutée aux adresses figurant dans Liste noire (expéditeurs) 226. Comme pour l'option ci-dessus, relative à la liste blanche, il n'est pas évident qu'un message provenant ou à destination d'une adresse inscrite sur la liste noire du Filtre anti-spam soit considéré comme du spam. C'est pourquoi la valeur indiquée dans le champ de cette option sera ajoutée au score du message qui sera ensuite utilisé pour déterminer si le message est indésirable ou non.

Toute correspondance trouvée par la vérification DNS-BL ajoute ces points au score
Si vous utilisez les Listes noires DNS 231 saisissez dans ce champ une valeur qui sera ajoutée au score d'un message si la vérification trouve une correspondance. Parfois, l'analyse heuristique du Filtre anti-spam n'attribue pas un score assez élevé à un message pour qu'il soit considéré comme indésirable, tandis que la vérification DNS-BL l'identifie comme pouvant être du spam. Ainsi, en ajoutant cette valeur au score de ce type de message, le nombre de spams qui parviennent à passer entre les mailles du Filtre anti-spam peut être réduit.

4.3.2 Listes noires DNS (DNS-BL)

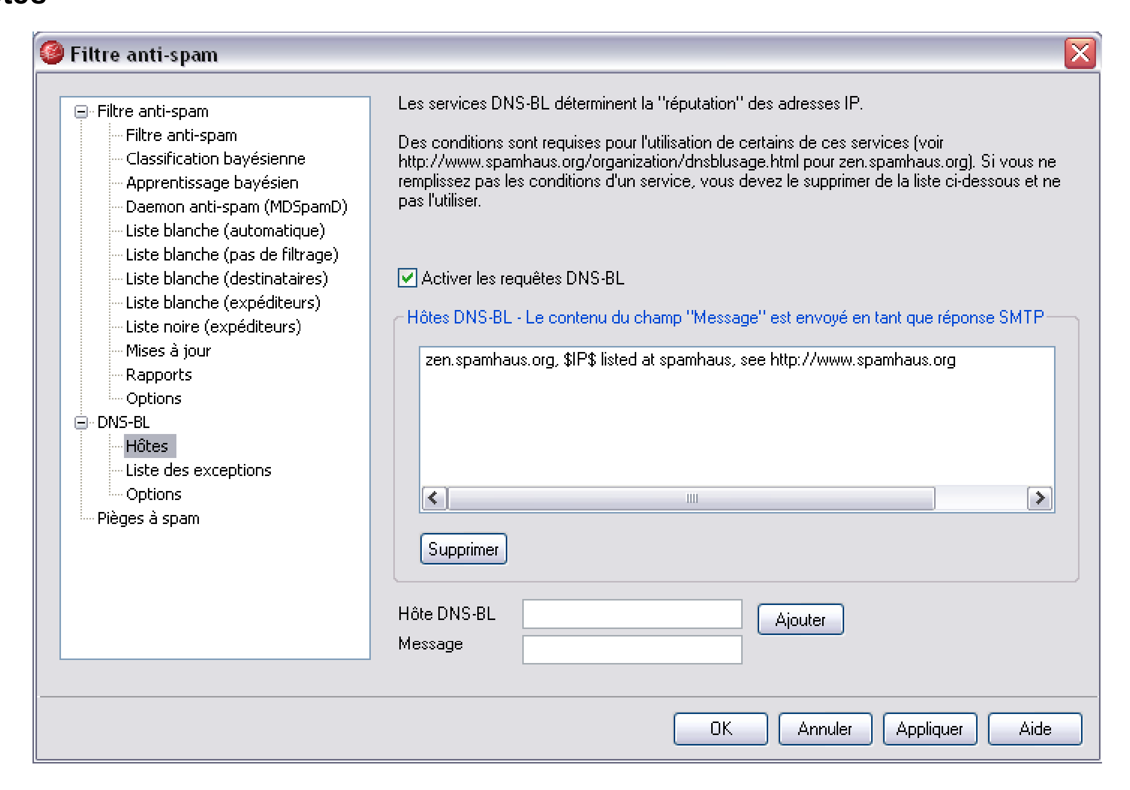
Cette fonctionnalité permet de vérifier si les expéditeurs des messages reçus ne figurent pas sur des listes noires DNS (listes de serveurs connus pour envoyer du spam). Si l'IP connectée figure sur une de ces listes, le message est refusé, mis en quarantaine, ou marqué comme spam ; en fonction des paramètres définis dans l'onglet Options 234.

Cet outil inclut une liste blanche permettant de ne pas soumettre certaines adresses IP aux vérifications DNS-BL. Avant de l'activer, ajoutez votre plage d'adresses IP locales à la liste blanche pour éviter qu'elles ne soient vérifiées. 127.0.0.1 figure déjà dans cette liste.

Voir également :

Hôtes DNS-BL 232
Options DNS-BL 234
Liste blanche DNS-BL 233

4.3.2.1 Hôtes



Hôtes DNS-BL

Activer les requêtes DNSBL
Le moteur DNSBL interroge les hôtes ci-dessous afin de savoir si l'adresse IP d'une connexion SMTP entrante figure sur une liste noire de spammeurs. Si un hôte indique qu'une adresse IP est sur une liste noire, le message peut être refusé, mis en quarantaine ou marqué comme spam (un texte est ajouté dans l'objet) ; en fonction des paramètres définis dans l'onglet Options 234.

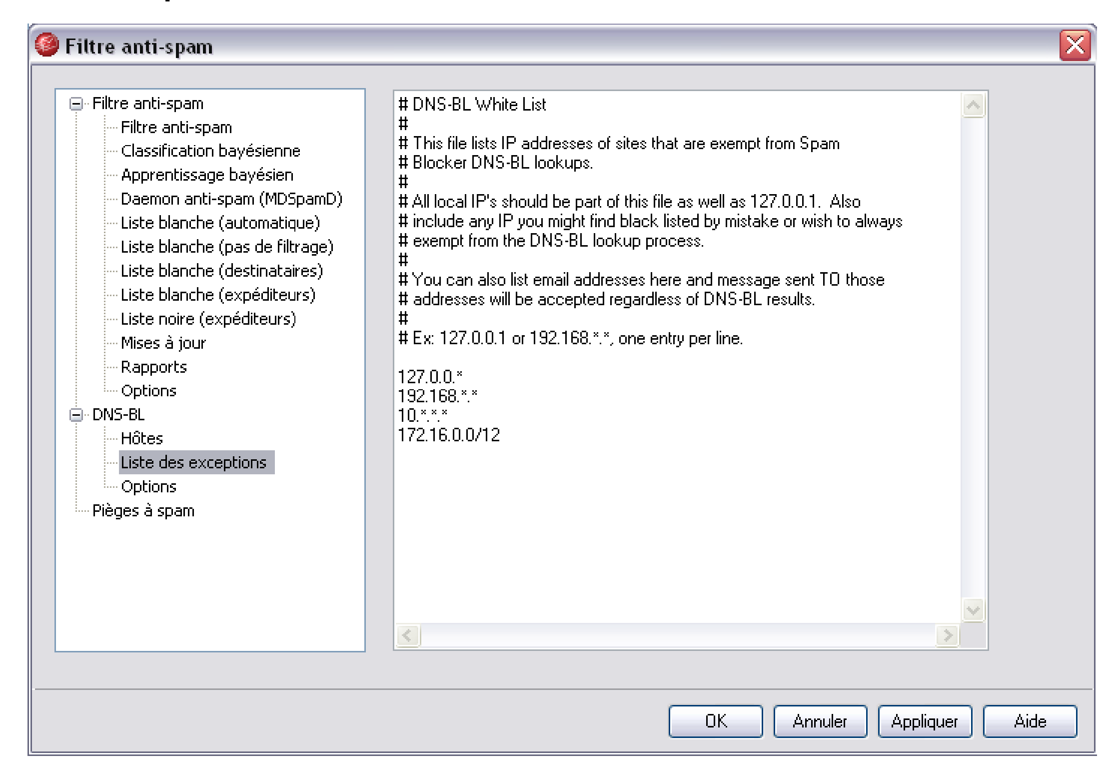
Supprimer
Pour supprimer un hôte de la liste, sélectionnez-le et cliquez sur ce bouton.

Hôte DNS-BL
Pour ajouter un hôte à la liste, indiquez ici son nom (par ex. : zen.spamhaus.org), indiquez un message à renvoyer en cas de refus (facultatif), puis cliquez sur le bouton *Ajouter*.

Message
Lorsqu'un message est refusé, il est possible d'envoyer un message personnalisé à l'expéditeur afin de lui indiquer les raisons de ce refus (sinon, la réponse "utilisateur inconnu" est envoyée automatiquement). Pour cela, indiquez ici le message de votre choix et activez l'option *Lorsqu'un message est rejeté envoyer le contenu du champ Message plutôt que 'Utilisateur inconnu'* dans l'onglet Options234.

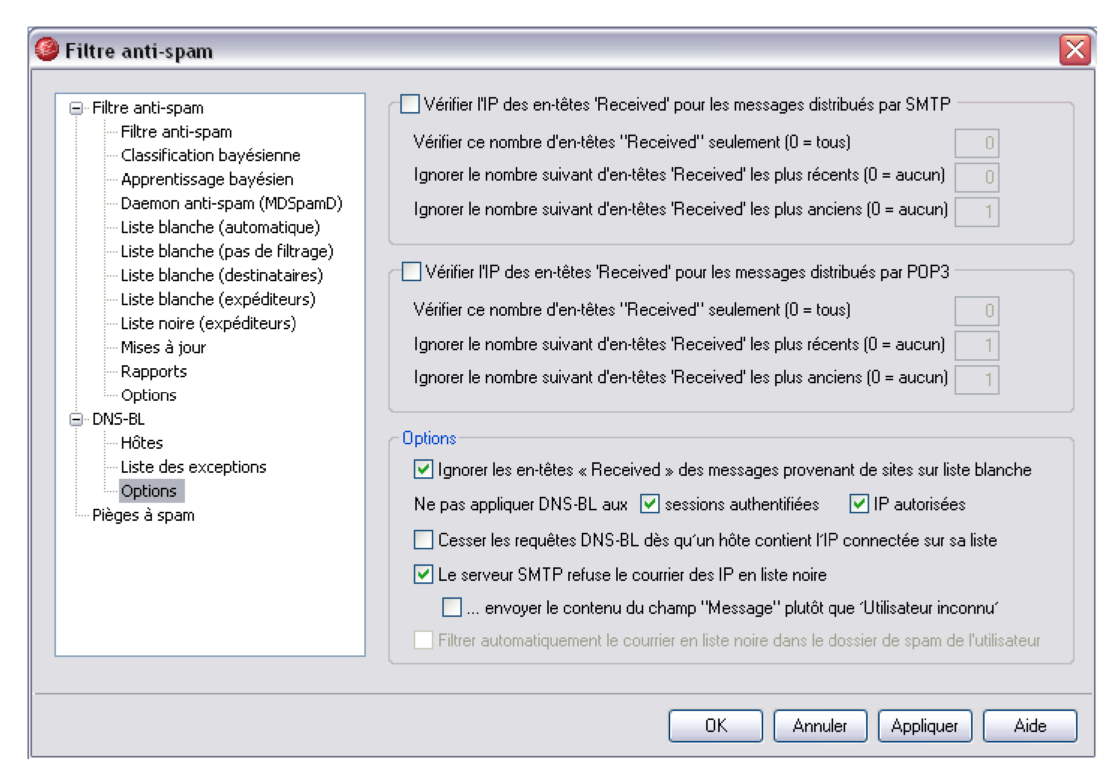
Ajouter
Après avoir indiqué un hôte et un message à renvoyer, cliquez sur ce bouton pour l'ajouter à la liste des hôtes DNS-BL.

4.3.2.2 Liste des exceptions



Cet onglet vous permet de définir les adresses IP dispensées des vérifications DNS-BL. Vous devez toujours inclure à la liste l'ensemble de vos adresses IP locales pour ne pas que les messages provenant de domaines ou d'utilisateurs locaux soient vérifiés (c'est-à-dire 127.0.0.*, 192.168.*.*, etc.). Inscrivez une adresse par ligne ; les caractères jokers sont acceptés.

4.3.2.3 Options



Vérifier l'IP des en-têtes "Received" pour les messages collectés avec SMTP
Activez ce paramètre si vous voulez que les listes noires DNS vérifient l'adresse IP contenue dans les en-têtes Received des messages reçus par SMTP.

Vérifier ce nombre d'en-têtes seulement (0 =tous)
Indiquez le nombre d'en-têtes "Received" que les listes noires DNS doivent vérifier en commençant par le plus récent. La valeur "0" signifie que tous les en-têtes Received seront vérifiés.

Ignorer le nombre suivant d'en-têtes "Received" les plus récents (0 = aucun)
Utilisez cette option si vous souhaitez que les listes noires DNS ignorent un ou plusieurs en-têtes Received lorsqu'il vérifie les messages SMTP. Cette option est configurée à "1" par défaut car il est souvent nécessaire d'ignorer l'en-tête Received le plus récent.

Ignorer le nombre suivant d'en-têtes "Received" les plus anciens (0 = aucun)
Utilisez cette option si vous souhaitez que les listes noires DNS ignorent un ou plusieurs en-têtes Received les plus anciens lorsqu'il vérifie les messages SMTP.

Vérifier l'IP des en-têtes 'Received' pour les messages distribués par POP3
Lorsque ce paramètre est activé, le système DNS-BL vérifie l'adresse IP contenue dans les en-têtes Received des messages collectés via DomainPOP ou MultiPOP.

Vérifier ce nombre d'en-têtes seulement (0 =tous)
Indiquez le nombre d'en-têtes "Received" que les listes noires DNS doivent

vérifier en commençant par le plus récent. La valeur "0" signifie que tous les en-têtes Received seront vérifiés.

Ignorer le nombre suivant d'en-têtes "Received" les plus récents (0 = aucun)
Utilisez cette option si vous souhaitez que les listes noires DNS ignorent un ou plusieurs en-têtes Received lors de la vérification des messages collectés via DomainPOP ou MultiPOP. Cette option est configurée à "1" par défaut car il est souvent nécessaire d'ignorer l'en-tête Received le plus récent.

Ignorer le nombre suivant d'en-têtes "Received" les plus anciens (0 = aucun)
Utilisez cette option si vous souhaitez que les listes noires DNS ignorent un ou plusieurs en-têtes Received les plus anciens lorsqu'il vérifie les messages DomainPOP et MultiPOP.

Options

Ignorer les en-têtes "Received" des messages provenant de sites sur liste blanche
Lorsque cette option est activée, les listes DNS ne vérifient pas les en-têtes "Received" dans les messages provenant d'adresses IP que vous avez inscrites sur liste blanche. Allez dans l'onglet Liste des exceptions 233 pour indiquer ces adresses IP.

Ne pas appliqer DNS-BL aux :

sessions authentifiées
Si vous activez cette option, les sessions ayant été authentifiées à l'aide de la commande AUTH seront dispensées de vérification DNS-BL.

IP autorisées
Cochez cette case pour que les adresses figurant dans l'onglet Hôtes autorisés 246 soient dispensées de vérification.

Cesser les requêtes DNSBL dès qu'un hôte contient l'IP connectée sur sa liste
Les en-têtes d'un message contiennent souvent plusieurs adresses IP ; et plusieurs hôtes sont interrogés pour chacune d'entre elles. Par défaut, MDaemon arrête d'envoyer des requêtes aux hôtes DNSBL dès qu'une IP en liste noire est trouvée. Désactivez cette option si vous souhaitez continuer à effectuer des requêtes pour toutes les adresses et sur tous les hôtes, même si une correspondance a été trouvée.

Le serveur SMTP refuse le courrier des IP en liste noire
Lorsque cette option est activée, MDaemon refuse les messages dont l'expéditeur figure sur liste noire. Si vous désactivez cette option, ces messages ne sont pas refusés, mais un en-tête X-MDDNSBL-Result est inséré. Il est ensuite possible de filtrer les messages contenant cet en-tête à l'aide de règles du Filtre de contenu. De plus, si vous n'activez pas cette option, il est toutefois possible d'utiliser l'option *Filtrer automatiquement le courrier en liste noire dans le dossier spam de l'utilisateur*, ou bien de laisser le Filtre anti-spam ajuster le score du message.



Cette fonctionnalité bloque un grand nombre de spams ; cependant, certains sont parfois mis en liste noire par erreur. Il est donc déconseillé de refuser directement les messages.

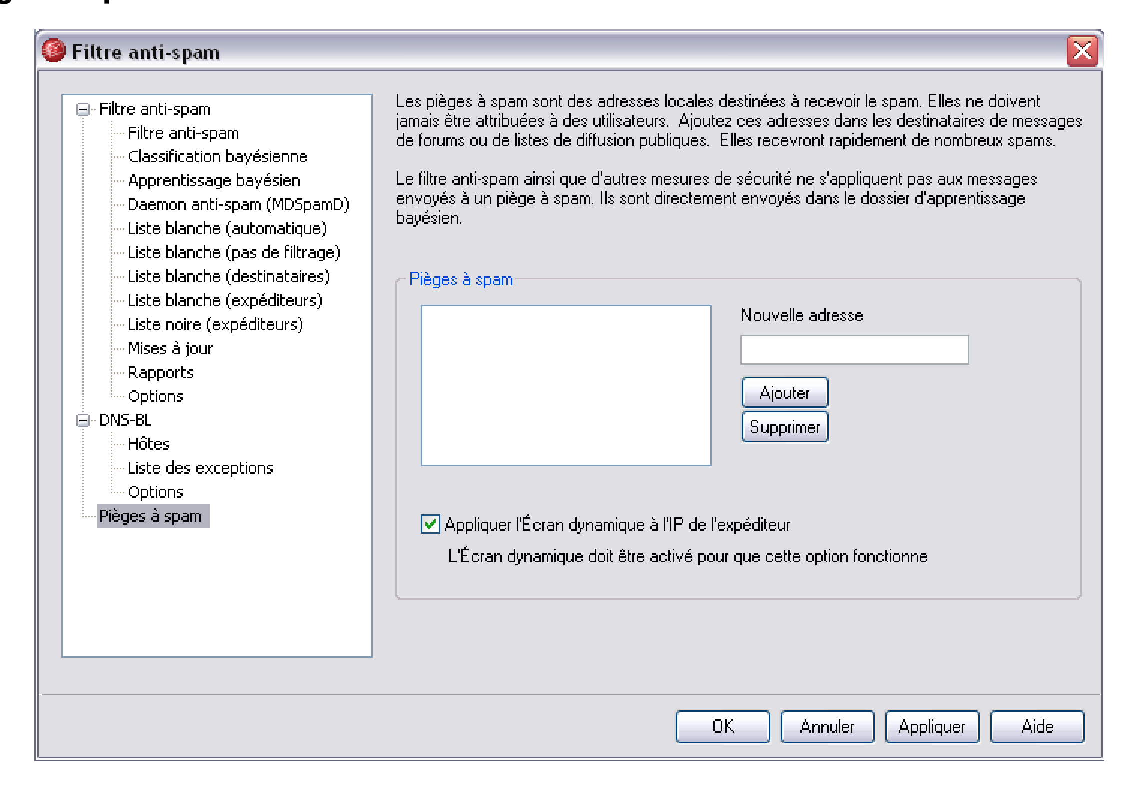
...envoyer le contenu du message plutôt que 'Utilisateur inconnu'
Cochez cette case si vous voulez qu'un message particulier, associé à un serveur de liste noire, soit envoyé lors d'une session SMTP à chaque fois qu'une adresse IP inscrite sur liste noire est trouvée. Sinon, le message "Utilisateur inconnu" est envoyé. Cette option n'est disponible que si vous avez coché la précédente.

Filtrer automatiquement le courrier en liste noire dans le dossier spam de l'utilisateur
En sélectionnant cette option, un dossier IMAP "Junk E-mail" est créé pour chaque compte utilisateur que vous ajouterez dans MDaemon. Pour chacun d'eux, MDaemon crée également un filtre de courrier qui recherche les en-têtes X-MDDNSBL-Result et envoie les messages contenant ces en-têtes dans le dossier spam des utilisateurs. Au moment où vous cochez cette case, MDaemon demande si vous souhaitez créer ce dossier et ce filtre pour les comptes utilisateurs déjà existants (voir ci-dessous).

Générer automatiquement un filtre et un dossier Spam pour chaque compte

MDaemon peut créer automatiquement un dossier de courrier IMAP "Junk E-mail" pour chaque compte, et générer un filtre qui entraînera l'enregistrement des messages contenant l'en-tête X-MDDNSBL-Result dans ce dossier IMAP. Lorsque vous sélectionnez l'option *Filtrer automatiquement le courrier en liste noire dans le dossier spam de l'utilisateur*, une boîte de dialogue s'ouvre et vous propose la création du filtre et du dossier IMAP pour tous les comptes. Cliquez sur "Oui" pour créer ces deux éléments. Bien qu'elle ne soit pas infaillible, cette méthode est une façon simple et généralement fiable d'identifier rapidement les messages indésirables ; cela évite au spam de se mêler au courrier légitime des utilisateurs. Ceux-ci n'auront qu'à vérifier de temps à autre le contenu de leur dossier de spam pour s'assurer que des messages importants n'y ont pas été enregistrés par erreur (cela peut arriver). Si, au moment de créer les dossiers et les filtres pour chaque compte, MDaemon s'aperçoit que l'un d'entre eux possède déjà un filtre qui vérifie la présence des en-têtes X-RBL-Warning, aucun changement ne sera effectué. Si vous ne souhaitez pas conserver le nom "Junk E-mail" du dossier IMAP, vous disposez d'une option dans l'onglet Système159 dans Configuration » Préférences.

4.3.3 Pièges à spam



Les pièges à spam (Sécurité » Filtre anti-spam » Pièges à spam) sont des adresses e-mail locales destinées à collecter des spams. Ces adresses ne correspondent pas à des comptes ou des alias valides et ne doivent jamais être utilisées pour envoyer ou recevoir du courrier légitime. Une fois créées, exposez-les publiquement en les ajoutant dans un message de forum ou d'une liste de diffusion publique et elles recevront rapidement de nombreux spams. Vous pouvez également récupérer les adresses locales invalides ayant reçu des spams et les utiliser dans cette liste. Ces adresses ne recevant jamais de courrier légitime, tous les messages qui leur sont adressés sont directement transférés dans le dossier d'apprentissage bayésien. De plus, il est possible de bloquer les futures connexions de l'IP de l'expéditeur à l'aide de l'Écran dynamique. Toutes ces mesures ont pour but d'améliorer l'identification et le blocage des spams.

Pièges à spam

Liste des adresses que vous avez choisies pour utiliser en tant que pièges à spam.

Nouvelle adresse
Pour ajouter une adresse à la liste, saisissez son nom dans ce champ et cliquez sur *Ajouter*.

Supprimer
Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur ce bouton.

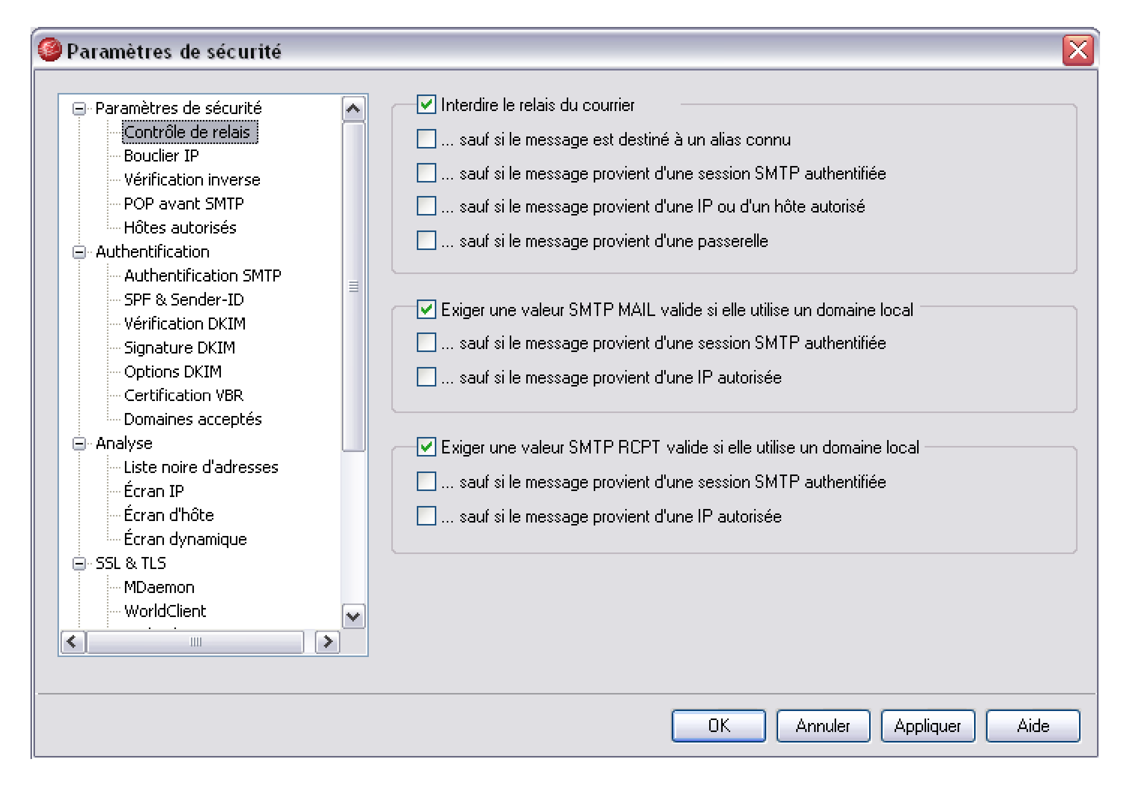
Appliquer l'Écran dynamique à l'IP de l'expéditeur
Cochez cette case si vous souhaitez appliquer l'Écran dynamique 269 aux IP ayant envoyé des messages aux adresses de piège à spam. Pour cela, l'Écran dynamique

doit être activé.

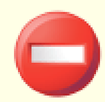
4.4 Paramètres de sécurité

4.4.1 Paramètres de sécurité

4.4.1.1 Contrôle de relais



Cliquez sur Sécurité » Paramètres de sécurité » Contrôle du relais pour définir la façon dont votre serveur doit réagir face au relais du courrier. Lorsqu'un message arrive sur votre serveur de messagerie et qu'il ne provient pas ou n'est pas destiné à une adresse locale, votre serveur est chargé de relayer (ou de distribuer) ce message pour le compte d'un autre utilisateur. Si vous ne voulez pas que votre serveur relaie le courrier pour des utilisateurs inconnus, vous pouvez utiliser les paramètres de cette boîte de dialogue.



En relayant du courrier pour d'autres serveurs sans faire de distinction, votre domaine peut être mis sur liste noire par un ou plusieurs services DNS-BL 231. Le relais ouvert est fortement déconseillé car les "spammeurs" exploitent les serveurs ouverts pour ne pas laisser de trace.

Relais du courrier

Interdire le relais du courrier
Lorsque cette option est activée, MDaemon refuse de distribuer les messages si l'expéditeur ET le destinataire ne sont pas des utilisateurs locaux.

...sauf si le message est destiné à un alias connu
Lorsque cette option est activée, MDaemon relaie le courrier destiné à des aliases 347 d'adresses.

...sauf si le message provient d'une session SMTP authentifiée
Lorsque cette option est activée, MDaemon relaie toujours le courrier lorsqu'il est envoyé via une session SMTP authentifiée.

...sauf si le message provient d'une IP ou d'un hôte autorisé
Cochez cette option si vous souhaitez autoriser le relais du courrier provenant d'une adresse IP ou d'un hôte autorisé.

...sauf si le message provient d'une passerelle
Activez cette option si vous voulez que MDaemon permette le relais de courrier à travers des passerelles de domaine, sans tenir compte de vos paramètres de relais. Cette fonctionnalité, désactivée par défaut, n'est pas recommandée.

Vérification des comptes

Exiger une valeur SMTP MAIL valide si elle utilise un domaine local
Cochez cette option si vous souhaitez vérifier que la valeur MAIL transmise lors de la session SMTP correspond à un compte valide lorsqu'elle indique qu'elle appartient à une passerelle ou un domaine local.

...sauf si le message provient d'une session SMTP authentifiée
Cochez cette case si vous souhaitez que l'option ci-dessus ne s'applique pas aux messages provenant de sessions authentifiées.

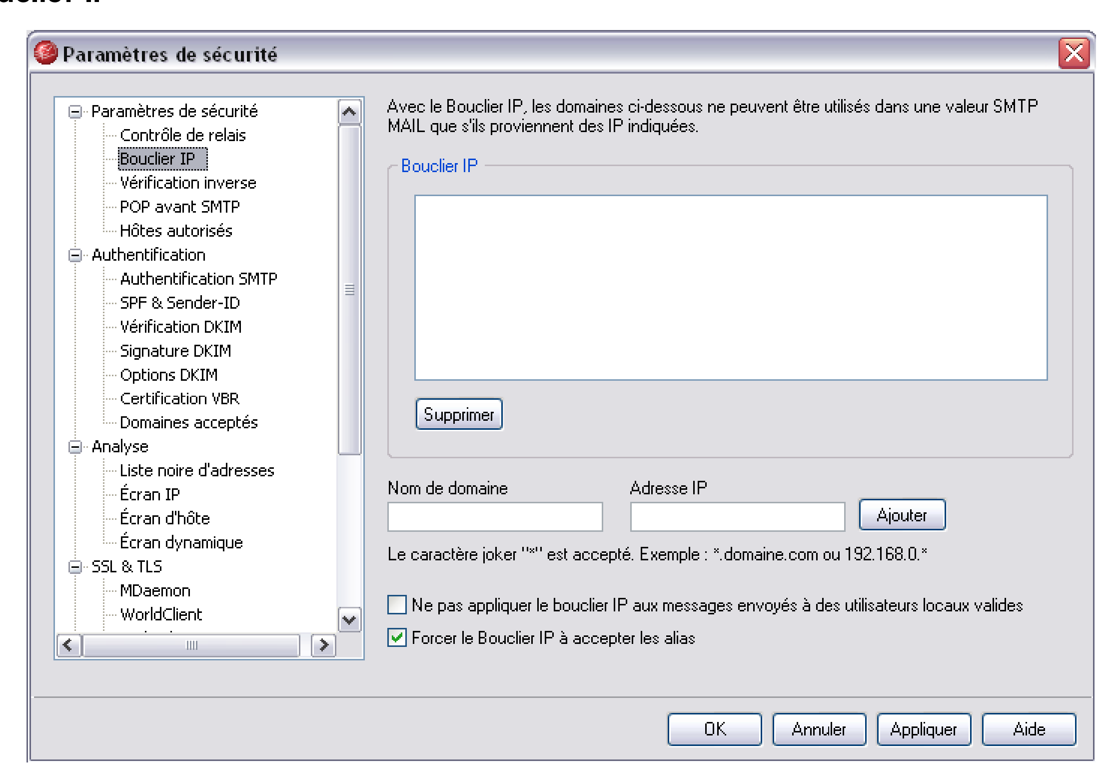
...sauf si le message provient d'une IP autorisée
Cochez cette case si vous souhaitez que l'option ci-dessus ne s'applique pas aux messages provenant d'adresses IP autorisées.

Exiger une valeur SMTP RCPT valide si elle utilise un domaine local
Cochez cette option si vous souhaitez vérifier que la valeur RCPT transmise lors de la session SMTP correspond à un compte valide lorsqu'elle indique qu'elle appartient à une passerelle ou un domaine local.

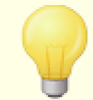
...sauf si le message provient d'une session SMTP authentifiée
Cochez cette case si vous souhaitez que l'option ci-dessus ne s'applique pas aux messages provenant de sessions authentifiées.

...sauf si le message provient d'une IP autorisée
Cochez cette case si vous souhaitez que l'option ci-dessus ne s'applique pas aux messages provenant d'adresses IP autorisées.

4.4.1.2 Bouclier IP



Situé dans Sécurité » Paramètres de sécurité le Bouclier IP est une liste de combinaisons domaine/adresse IP qui seront vérifiés lors de la réception de la commande SMTP MAIL FROM:. Une session SMTP, ouverte par une personne qui prétend faire partie d'un des domaines répertoriés, sera acceptée uniquement si elle provient d'un ordinateur dont l'adresse IP figure dans cette liste. Par exemple, supposons que votre nom de domaine soit mdaemon.com et que vos ordinateurs locaux utilisent des adresses IP comprises entre 192.168.0.0 et 192.168.0.255. Avec ces informations, vous pouvez configurer le bouclier IP pour qu'il associe le nom de domaine mdaemon.com avec la plage d'adresses IP 192.168.0.* (les caractères jokers sont autorisés). Ainsi, chaque fois qu'un ordinateur se connecte à votre serveur SMTP et déclare "MAIL FROM someone@mdaemon.com", la session SMTP ne continue que si l'ordinateur en question possède une adresse IP comprise entre 192.168.0.0 et 192.168.0.255.



Il est possible de ne pas appliquer ces restrictions aux sessions authentifiées à l'aide d'une option située dans Authentification SMTP 247.

Bouclier IP

Il s'agit de la liste des combinaisons des domaines et de leurs adresses IP qui seront comparées lorsqu'un serveur tente de se connecter à SecurityGateway et prétend appartenir à l'un de ces domaines. Dans ce cas, l'adresse IP du serveur expéditeur doit

correspondre au domaine indiqué.

Nom de domaine
Nom de domaine à ajouter à la liste.

Adresse IP
Adresse IP (ou plage d'adresses) associée au nom de domaine ci-dessus. Lorsqu'un message prétend provenir de ce domaine, l'adresse IP du serveur expéditeur doit correspondre à celle saisie dans ce champ. (Elle doit être saisie sous forme décimale séparée par des points.)

Ajouter
Cliquez sur le bouton Ajouter pour ajouter le domaine et la plage d'adresses IP à la liste.

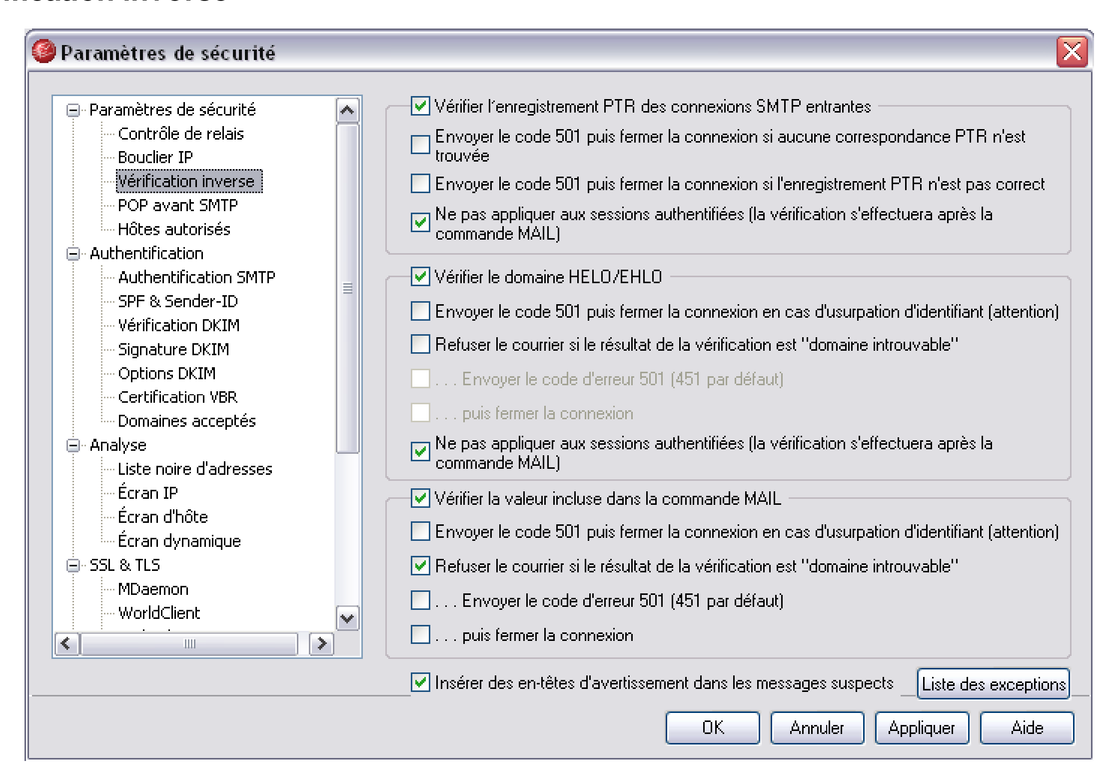
Supprimer
Pour supprimer une entrée de la liste, sélectionnez-la et cliquez sur ce bouton.

Ne pas appliquer le bouclier IP aux messages envoyés à des utilisateurs locaux valides
Sélectionnez cette option si vous voulez que seuls les messages destinés à un utilisateur non local ou à un utilisateur local non valide soient soumis à la correspondance domaine/IP. Ce système évite que d'autres personnes, prétendant être des utilisateurs locaux, puissent transmettre leur courrier via votre serveur. Il permet également d'économiser des ressources car il ne vérifie pas les expéditeurs qui envoient du courrier à des utilisateurs sur votre serveur. Si vous sélectionnez à la fois cette option et celle située en dessous *Forcer le boulier IP à accepter les alias*, les messages adressés à des alias valides seront également acceptés.

Forcer le boulier IP à accepter les alias
Sélectionnez cette option si vous souhaitez que le bouclier IP accepte les alias lorsqu'il vérifie les paires Domaines/adresses IP. Lorsqu'elle est activée, le bouclier convertit les alias en leurs noms de domaine réels pour ne pas bloquer le message s'il passe le bouclier avec succès. Si cette option n'est pas activée, le bouclier IP traite les alias comme des adresses indépendantes des comptes qu'ils représentent. Ainsi, si l'adresse IP d'un alias est bloquée par le bouclier IP, le courrier est refusé. Cette option se trouve aussi dans l'éditeur d'alias (onglet Options) 349.

Si vous souhaitez que les messages entrants adressés à des alias d'adresses valides soient dispensées de la vérification du bouclier IP, sélectionnez à la fois cette option et celle située au dessus.

4.4.1.3 Vérification inverse



En utilisant les options de cette boîte de dialogue, MDaemon peut être configuré pour effectuer une vérification inverse sur le domaine passé dans les commandes HELO/EHLO et/ou MAIL. Lors de ces vérifications, MDaemon essaie d'obtenir toutes les adresses IP des enregistrements MX et A pour le domaine donné. Ensuite, l'IP de l'ordinateur qui se connecte est comparée à cette liste afin de déterminer si l'expéditeur a falsifié ou non son identité.

Souvent, l'adresse IP du serveur qui envoie du courrier ne correspond à aucun enregistrement MX ou A connu pour le domaine donné mais distribue le courrier légitimement. La vérification inverse n'a donc pas pour objectif d'exclure du courrier mais d'inclure autant d'informations que possible dans les fichiers journaux, et de fournir les moyens par lesquels le postmaster peut agir en fonction de ses propres règles locales concernant les messages suspects. Dans ce but, une option existe et permet d'insérer un en-tête spécial dans tous les messages qui ne réussissent pas à franchir l'étape de la vérification inverse. Le système de filtre de contenu peut alors être utilisé pour déterminer le sort des messages contenant cet en-tête.

Vous pouvez également effectuer une vérification inverse sur des enregistrements PTR d'adresses IP entrantes. Lorsque vous utilisez cette option, la connexion peut être annulée ou un en-tête d'avertissement peut être inséré dans le courrier, si l'adresse IP entrante ne correspond à aucun enregistrement PTR.

Enfin, il est généralement admis que le fait d'accepter du courrier de sources qui s'identifient en utilisant un domaine qui n'existe pas devrait être optionnel. Par conséquent, il existe un paramètre qui vous permet de refuser des messages pour lesquels la vérification inverse a retourné un message "domaine introuvable" depuis le serveur DNS. Dans ce genre de cas, MDaemon retourne le code d'erreur 451, refuse le message, puis autorise la progression de la session SMTP en cours.

Toutefois, il est possible d’envoyer le code d’erreur 501, de fermer la connexion, ou d’effectuer les deux opérations à la fois. Pour cela, utilisez les paramètres correspondants.

Les adresses IP autorisées et l'adresse localhost (127.0.0.1) sont toujours dispensées de la vérification inverse.

Vérifier l’enregistrement PTR des connexions SMTP entrantes
Activez cette option si vous voulez que MDaemon effectue une vérification inverse sur l’enregistrement PTR de toutes les connexions SMTP entrantes.

Envoyer le code 501 puis fermer la connexion si aucune correspondance PTR n'est trouvée
Activez cette option pour que MDaemon envoie un code d’erreur 501 (erreur de syntaxe dans des paramètres ou arguments) et ferme la connexion si aucun enregistrement PTR n’est trouvé pour le domaine. Option à utiliser avec précaution.

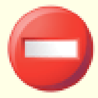
Envoyer le code 501 puis fermer la connexion si l’enregistrement PTR n'est pas correct
Activez cette option pour que MDaemon envoie un code erreur 501 (erreur de syntaxe dans des paramètres ou arguments) et ferme la connexion si le résultat de la vérification d’un enregistrement PTR ne correspond pas.

Ne pas appliquer aux sessions authentifiées (la vérification s’effectuera après la commande MAIL)
Lorsque cette option est activée, la vérification PTR des connexions SMTP entrantes ne s’effectue qu’après la commande MAIL, afin de déterminer si la session est authentifiée.

Vérifier le domaine HELO/EHLO
Activez cette option si vous voulez qu’une vérification soit effectuée sur le nom de domaine communiqué lors du dialogue HELO/EHLO de la session. La commande HELO/EHLO est utilisée par le client (l’ordinateur qui envoie) pour s’identifier sur le serveur. Le nom de domaine, envoyé par le client dans cette commande, est utilisé par le serveur pour remplir le champ from de l’en-tête Received.

Vérifier la valeur incluse dans la commande MAIL
En activant ce paramètre, une vérification est effectuée sur le nom de domaine communiqué durant l’envoi de la commande MAIL pour la transaction de courrier. L’adresse incluse dans la commande MAIL correspond au chemin inverse du message : il s’agit en principe de la boîte aux lettres d’envoi.Cependant, il peut parfois s’agir de l’adresse à laquelle envoyer les messages d’erreur.

Envoyer le code d’erreur 501 puis fermer la connexion en cas d’usurpation d’identifiant (attention)
Cochez cette case si vous voulez que le code d’erreur 501 soit envoyé et que la connexion soit ensuite fermée lorsque la vérification permet de déceler une usurpation d’identification.



Lorsque le résultat d'une vérification indique que le serveur utilise des informations d'identification usurpées, il est possible que ce résultat soit en réalité erroné. Il est fréquent pour les serveurs de messagerie de s'identifier à l'aide de valeurs qui ne correspondent pas à leur adresse IP. Cela peut être dû aux limitations et restrictions imposées par les FAI ou à d'autres raisons tout à fait légitimes. Pour cela, vous devez faire attention lorsque vous activez cette option. Il est probable que son utilisation entraîne le refus de messages légitimes de la part de votre serveur.

Refuser le courrier si le résultat de la vérification est "domaine introuvable"
Lorsqu'une vérification retourne le message "domaine introuvable", en activant cette option, le message sera refusé et le code d'erreur 451 (Action arrêtée : erreur de traitement) sera envoyé et la session sera alors autorisée à fonctionner normalement jusqu'à ce qu'elle soit terminée.

. . . envoyer le code d'erreur 501 (451 par défaut)
Activez cette option si vous voulez que le code d'erreur 501 (erreur de syntaxe dans des paramètres ou arguments) soit envoyé en réponse à un résultat "domaine introuvable", à la place du code 451.

. . . puis fermer la connexion
Activez cette option si vous voulez que la connexion soit fermée immédiatement, au lieu de continuer normalement, lorsque le résultat de la vérification inverse correspond à "domaine introuvable".

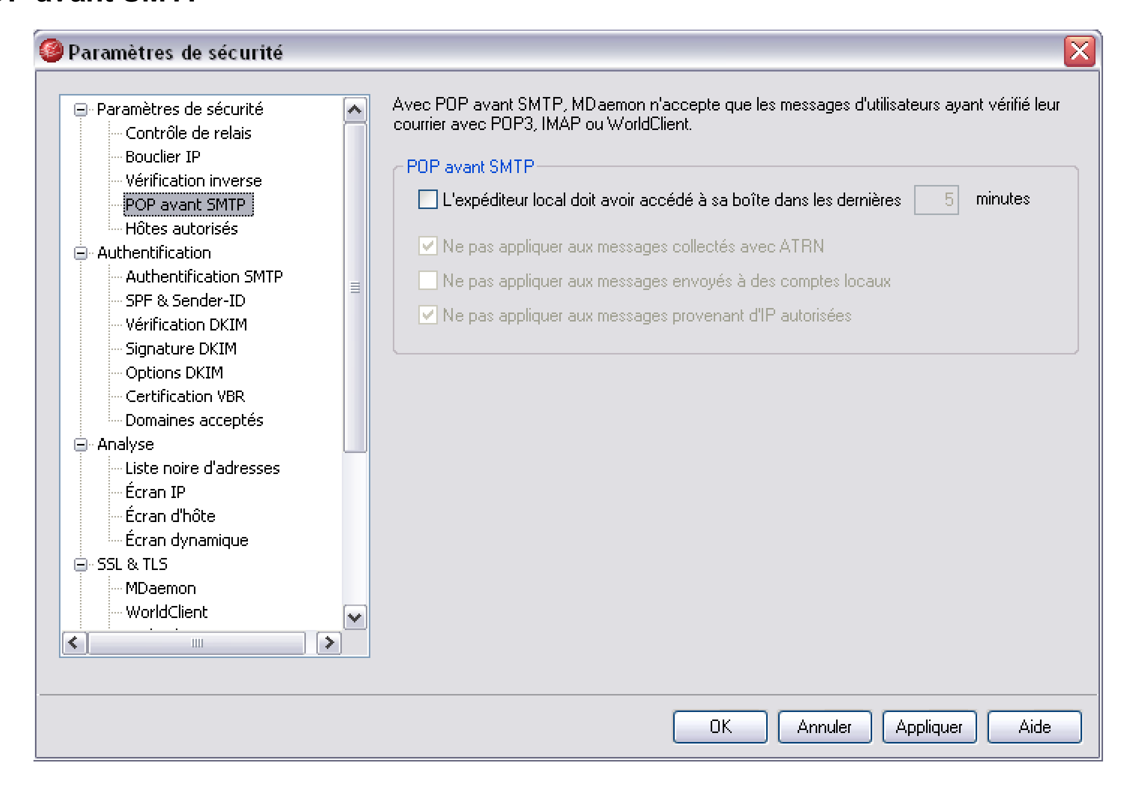
Insérer des en-têtes d'avertissement dans les mssages suspects
Activez cette option si vous voulez qu'un en-tête soit inséré dans les messages considérés comme suspects en raison des résultats de la vérification inverse. Vous pouvez changer le nom et le contenu de cet en-tête en modifiant le fichier MDaemon.ini comme suit :

```
[Special]
LookupWarningHeader=X-Lookup-Warning: text
```

Si vous modifiez cette valeur, MDaemon vous autorisera à remplacer la section "X-LookupWarning: text" par le texte de votre choix. Veillez cependant à ce que vos modifications soient conformes aux réglementations RFC relatives aux en-têtes de messages.

Liste des exceptions
Cliquez sur ce bouton pour définir la liste des adresses IP dispensées de vérification inverse.

4.4.1.4 POP avant SMTP



POP avant SMTP

L'expéditeur local doit avoir accédé à sa boîte dans les dernières XX minutes
Lorsque cette option est activée, les messages provenant d'utilisateurs locaux ne sont envoyés que si l'utilisateur s'est connecté à sa boîte aux lettres pendant la période indiquée.

Ne pas appliquer aux messages collectés via ATRN
Avec cette option, les messages collectés via ATRN 414 ne sont pas traités par la fonction POP avant SMTP.

Ne pas appliquer aux messages envoyés à des comptes locaux
Cochez cette case si vous souhaitez que cette restriction ne s'applique pas aux messages envoyés d'un utilisateur local à un autre. MDaemon exécute généralement la fonction POP avant SMTP dès que l'expéditeur est connu mais lorsque cette option est activée, il attend que le destinataire du message soit connu avant de déterminer si elle est nécessaire.

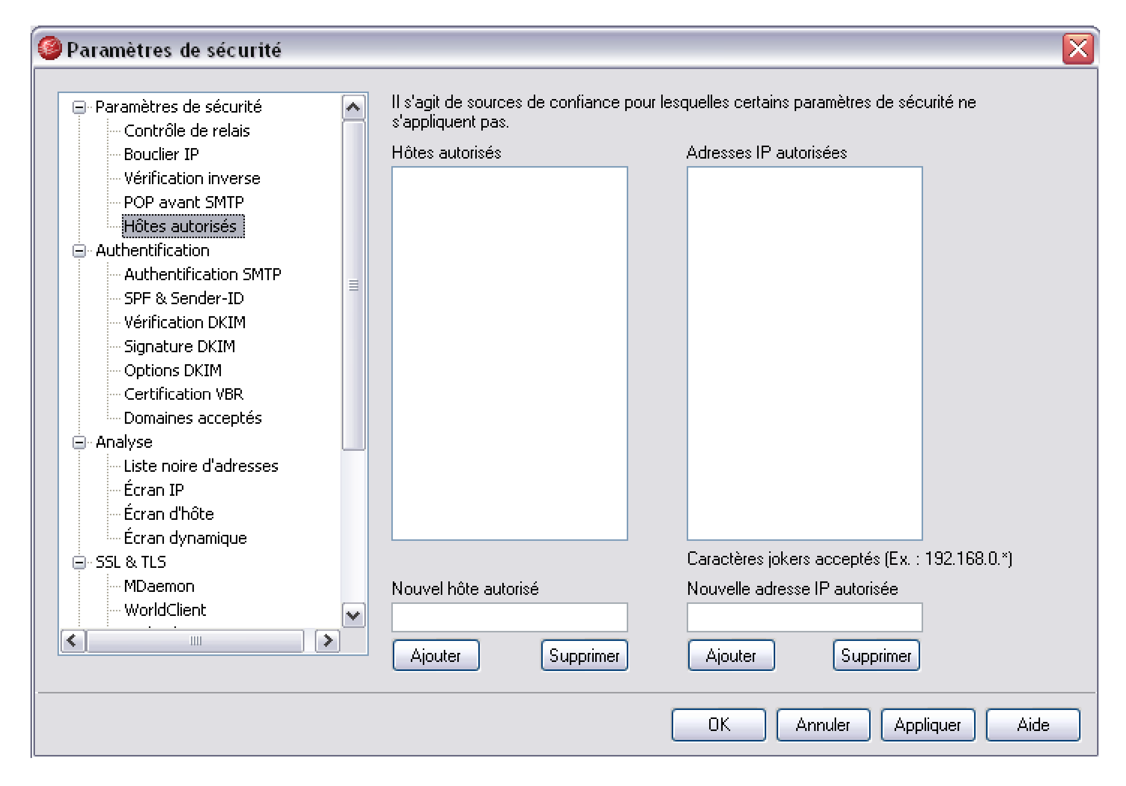
Ne pas appliquer aux messages provenant d'IP autorisées
Lorsque cette option est activée, cette restriction ne s'applique pas aux messages provenant d'adresses IP figurant dans la liste Hôtes autorisés 246.



Il est possible de ne pas appliquer POP avant SMTP aux sessions authentifiées à l'aide d'une option figurant dans

Authentification SMTP 247.

4.4.1.5 Hôtes autorisés



Les domaines et adresses IP figurant dans cette liste sont dispensés de certaines vérifications de sécurité. En effet, diverses options de MDaemon ont la possibilité de ne pas s'appliquer aux "hôtes/IP autorisés". Cet onglet contient la liste des domaines et adresses auxquels ces options font référence.

Hôtes autorisés
Listes d'hôtes auxquels certaines vérifications de sécurité ne s'appliquent pas.

Nouvel hôte autorisé
Entrez un nouveau nom de domaine à ajouter dans la liste.

Ajouter
Cliquez sur ce bouton pour ajouter le nouveau domaine à la liste.

Supprimer
Pour supprimer un domaine de la liste, sélectionnez-le et cliquez sur ce bouton.

Adresses IP autorisées
Listes d'adresses IP auxquelles certaines vérifications de sécurité ne s'appliquent pas.

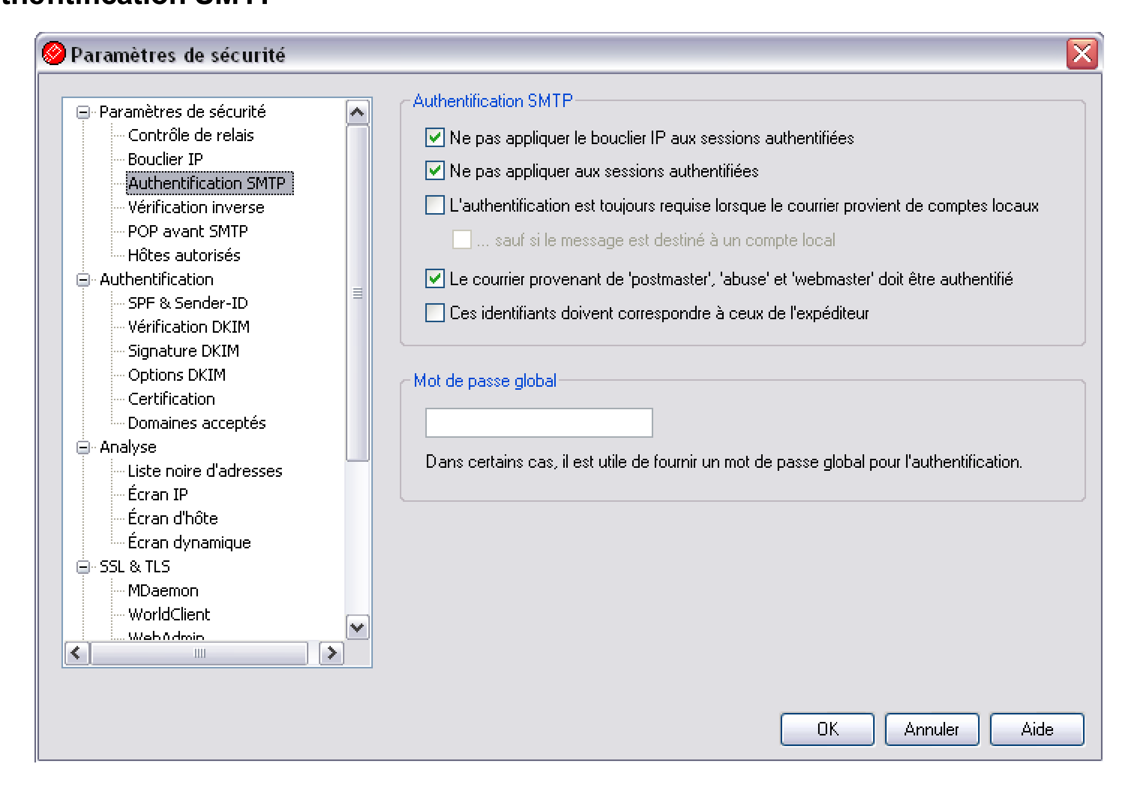
Nouvelle adresse IP autorisée
Entrez une adresse IP à ajouter dans la liste.

Ajouter
Cliquez sur ce bouton pour ajouter la nouvelle adresse à la liste.

Supprimer
Pour supprimer une IP de la liste, sélectionnez-la et cliquez sur ce bouton.

4.4.2 Authentification de l'expéditeur

4.4.2.1 Authentification SMTP



Authentification SMTP

Ne pas appliquer le bouclier IP aux sessions authentifiées
Lorsque cette option est activée, les restrictions du bouclier IP 240 ne s'appliquent pas aux utilisateurs authentifiés.

Ne pas appliquer POP avant SMTP aux sessions authentifiés
Lorsque cette option est activée, les restrictions de l'outil POP avant SMTP 245, ne s'appliquent pas aux utilisateurs authentifiés.

L'authentification est toujours requise lorsque le courrier provient de comptes locaux
Lorsque cette option est activée et qu'un message prétend appartenir à l'un des

domaines de MDaemon, le compte doit d'abord être authentifié. Dans le cas contraire, MDaemon refusera de distribuer le message.

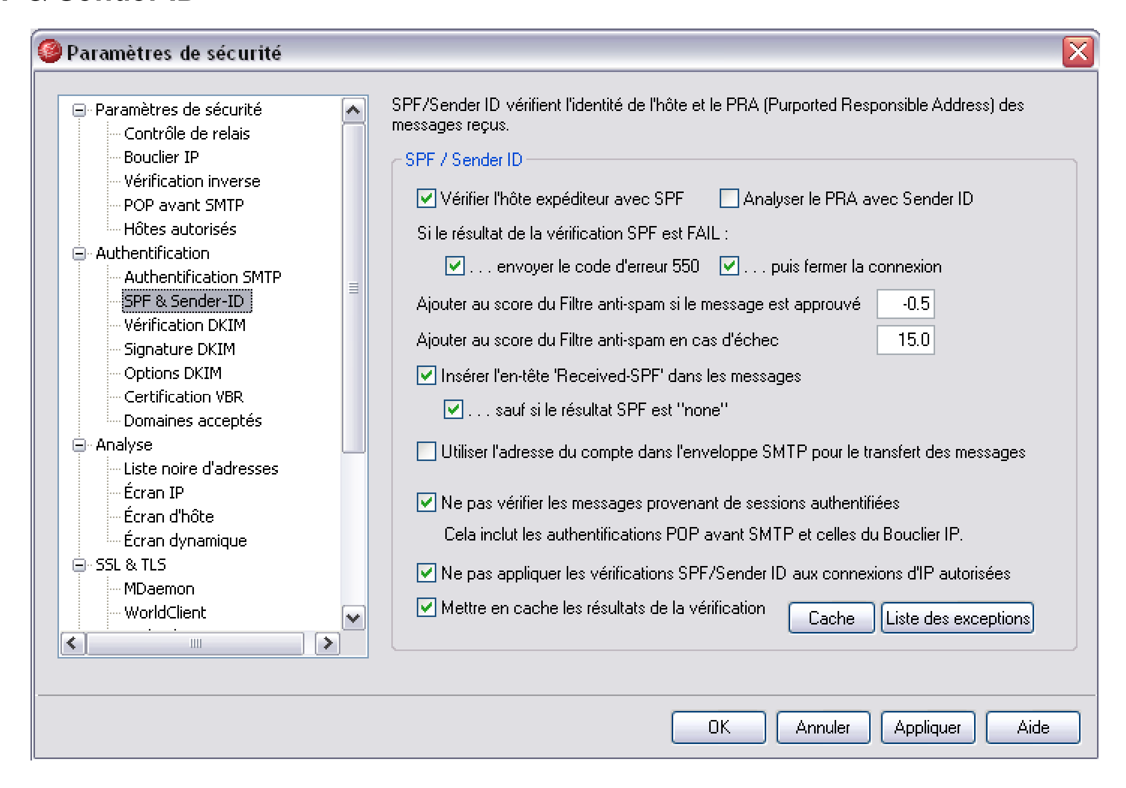
... sauf si le message est destiné à un compte local
Requiert l'authentification des messages provenant de comptes locaux, sauf si le destinataire est également un compte local. Remarque : cela peut s'avérer nécessaire lorsque vous exigez que certains utilisateurs emploient des serveurs différents pour le courrier entrant et sortant.

Le courrier provenant de 'Postmaster', 'abuse' et 'webmaster' doit être authentifié
Lorsqu'un message prétend provenir des comptes postmaster, abuse, ou webmaster de vos domaines locaux, une authentification est exigée par défaut. En effet, les spammeurs savent que ces comptes existent sur tous les serveurs et essaient de les utiliser pour envoyer du spam. Cette option est également affichée dans l'onglet Options 349 de l'éditeur d'alias.

Ces identifiants doivent correspondre à ceux de l'expéditeur
Activez cette option si vous souhaitez que les utilisateurs s'authentifiant lors de la distribution SMTP utilisent obligatoirement leurs propres informations d'authentification. L'identifiant et le mot de passe doivent correspondre à l'expéditeur indiqué dans la commande SMTP MAIL. Cela empêchera des utilisateurs locaux valides d'envoyer du courrier via votre système à partir d'une autre adresse que la leur.

Mot de passe global
Certaines configurations nécessitent un mot de passe global pour l'authentification. Si tel est le cas, indiquez-le ici.

4.4.2.2 SPF & Sender ID



MDaemon comporte deux systèmes de lutte contre l'usurpation d'adresse : Sender Policy Framework (SPF) et Sender ID qui permettent de vérifier l'identité de l'expéditeur d'un message.

La plupart des domaines publient dans les DNS des enregistrements MX indiquant les serveurs pouvant recevoir les messages qui leur sont destinés. Toutefois, ces enregistrements ne précisent pas quels serveurs peuvent envoyer des messages de la part du domaine. Avec SPF les domaines peuvent également publier des enregistrements permettant d'identifier les postes autorisés à envoyer des messages. En effectuant une vérification SPF sur les messages entrants, MDaemon essaie de déterminer si le serveur expéditeur est autorisé à envoyer des messages au nom du domaine correspondant, et ainsi de vérifier que l'adresse utilisée ne soit pas usurpée. Le système Sender ID est lié à SPF, mais il est plus complexe, afin de diminuer le risque d'erreurs.

Vous pouvez configurer les paramètres SPF et Sender ID de votre serveur à l'aide des options présentes sur cet onglet.

Plus d'informations sur SPF sont disponibles à l'adresse :

http://spf.pobox.com

Plus d'informations sur Sender ID sont disponibles à l'adresse :

http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

SPF / Sender ID

Vérifier l’hôte expéditeur avec SPF
Lorsque cette option est activée, MDaemon effectue des requêtes pour les données SPF de l’hôte expéditeur de tous les messages entrants, sauf ceux provenant d’adresses IP de la liste blanche, de sessions authentifiées, ou d’adresses IP autorisées (à condition que les options concernant ces exceptions soient activées). Les données vérifiées sont celles contenues dans la commande MAIL transmise lors de la session SMTP. Cette option est activée par défaut.

Analyser le PRA avec Sender ID
Lorsque cette option est activée, MDaemon analyse les en-têtes des messages reçus afin d’identifier le PRA (Purported Responsible Address) et ainsi déterminer l’origine du message.

Si le résultat de la vérification est FAIL :

...envoyer le code d’erreur 550
Un code d’erreur 550 est envoyé lorsque le résultat de la vérification SPF/Sender ID est "Fail".

...puis fermer la connexion
Avec cette option, la connexion est fermée immédiatement après l’envoi du code d’erreur 550.

Ajouter au score du Filtre anti-spam si le message est approuvé
Indiquez la valeur que vous souhaitez ajouter au score spam d’un message lorsqu’il provient d’un domaine figurant sur la liste des Domaines acceptés 264.



La valeur indiquée est généralement un nombre négatif afin que le score soit réduit pour les messages acceptés.

Ajouter au score du Filtre anti-spam en cas d’échec
Indiquez la valeur à ajouter au score du message lorsque la vérification échoue.

Insérer l’en-tête "Received-SPF" dans les messages
Cochez cette option pour ajouter un en-tête "Received-SPF" dans tous les messages.

...sauf si le résultat est "none"
Avec cette option l’en-tête "Received-SPF" n’est pas inséré dans les messages dont le résultat de la requête SPF est "none".

Utiliser l’adresse du compte dans l’enveloppe SMTP pour le transfert des messages
Cochez cette option si vous souhaitez que tous les messages transférés automatiquement par MDaemon utilisent l’adresse du compte local effectuant le transfert. Cela permet d’éviter bien des problèmes. En effet, les messages transférés comportent généralement l’adresse de l’expéditeur d’origine et non celle effectuant le transfert. Il est parfois nécessaire d’utiliser l’adresse locale afin d’éviter que le

serveur destinataire ne considère à tort que le message provient d'une adresse usurpée.

Options de vérification

Ne pas vérifier les messages provenant de sessions authentifiées
Les connexions authentifiées ne subissent pas de vérification SPF/Sender ID. Cela comprend les sessions vérifiées par Authentification SMTP 247, POP avant SMTP 245 ou le Bouclier IP 240.

Ne pas appliquer les vérifications SPF/Sender aux connexions d'IP autorisées
Activez cette option si vous souhaitez que ces vérifications ne s'appliquent pas aux connexions provenant d'adresses IP autorisées 246.

Mettre en cache les résultats de la vérification
Cochez cette option si vous souhaitez mettre temporairement en cache les résultats des vérifications SPF.

Cache
Ouvre le fichier du cache de SPF.

Liste des exceptions
Ouvre la liste blanche SPF ; ajoutez-y les adresses IP exemptes de vérification.

4.4.2.3 DomainKeys Identified Mail

DomainKeys et DKIM sont des systèmes de vérification cryptographiques qui permettent d'éviter l'usurpation des adresses e-mail. De plus, même s'ils n'ont pas été conçus dans ce but, ces outils facilitent la lutte contre le spam, car la plupart des spams proviennent d'une adresse usurpée. Enfin, ils vérifient l'intégrité des messages entrants et s'assurent qu'ils n'ont pas été altérés après avoir quitté le serveur de l'expéditeur. Par conséquent, DomainKeys et DKIM vous garantissent que les messages entrants proviennent de l'expéditeur indiqué et qu'ils n'ont pas été altérés au cours du transfert entre les serveurs.

DomainKeys/DKIM contrôlent la validité et l'intégrité des messages grâce à un système de paires de clés publiques et privées. Une clé publique cryptée est publiée dans les données DNS du serveur expéditeur, puis ce serveur attribue à chaque message sortant une signature contenant une clé privée chiffrée correspondante. De même, lorsque le serveur voit qu'un message entrant a été signé, il cherche la clé publique dans les données DNS du serveur expéditeur ; et la compare à la signature DomainKeys/DKIM du message. Si les clés ne correspondent pas, cela signifie qu'il s'agit d'une adresse usurpée ou que le message a été altéré. Le message est alors soit rejeté, soit accepté auquel cas son score spam est modifié.

Les paramètres pour la vérification des messages entrants se trouvent dans l'onglet Vérification DKIM 252, et pour les messages sortants, dans l'onglet Signature DKIM 255. D'autre part, en cliquant sur l'onglet *Sécurité* dans l'interface principale 22 de MDaemon, un onglet DomainKeys/DKIM permet de surveiller cette fonctionnalité en temps réel. Enfin, il est possible de conserver une trace de son activité dans :

Configuration » Serveur/domaines par défaut » Journalisation » Options.

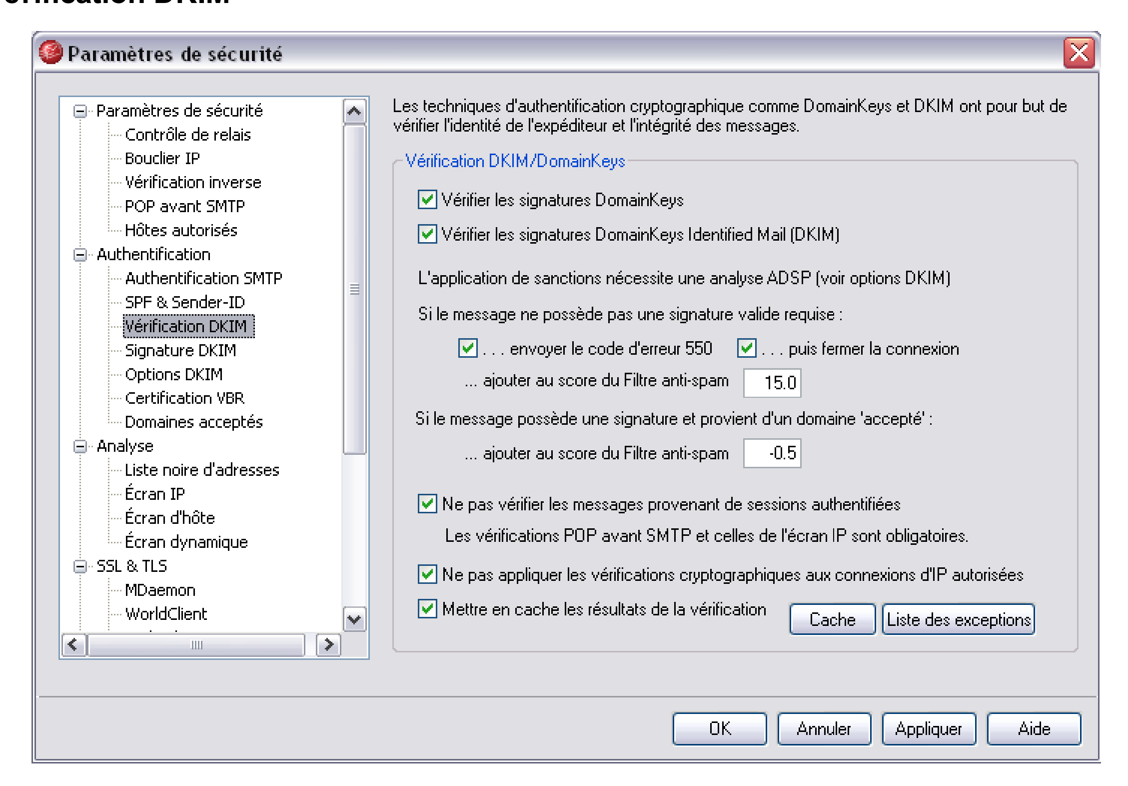
Voir également :

[Vérification DKIM](252)
[Signature DKIM](255)
[Options DKIM](258)

Pour en savoir plus sur DKIM, consultez le site : http://www.dkim.org/.

Pour en savoir plus sur DomainKeys, consultez le site : http://antispam.yahoo.com/domainkeys.

4.4.2.3.1 Vérification DKIM



Cet onglet contient les options de vérification des signatures DomainKeys (DK) et/ou DKIM dans les messages entrants. Lorsque cette fonctionnalité est activée et qu'un message entrant contient une signature cryptographique, MDaemon recherche la clé publique dans l'enregistrement DNS du domaine afin de déterminer la validité de cette signature.

Si la signature est valide, le traitement du message suit son cours normal. De plus, si le domaine de l'expéditeur figure dans l'onglet Domaines acceptés [264], cela a un effet positif sur le score de spam du message.

Si le message n’a pas de signature ou si la signature est invalide, MDaemon recherche l’enregistrement ADSP (Author Domain Signing Practices) du domaine dans l’en-tête From afin de déterminer si tous les messages de ce domaine doivent être signés ou bien si cela concerne uniquement une partie. Si l’enregistrement SSP indique qu’une signature valide est requise et que la clé publique indique qu’il ne s’agit pas d’un simple test de DKIM, la vérification échoue et le message est traité en conséquence : il peut être rejeté ou bien accepté en augmentant son score de spam.

Enfin, si l'enregistrement ADSP d'un site utilise une sytaxe inconnue à MDaemon, si aucun enregistrement n'existe, ou si l'option ADSP située dans les Options DKIM 258 est désactivée, aucune action punitive n'est effectuée. Les messages dont la signature est absente ou invalide sont traités comme le domaine ne signait qu'une partie de ses messages.

Plus d'informations sur DKIM sont disponibles à l'adresse : http://www.dkim.org/

Vérification DKIM/DomainKeys

Vérifier les signatures DomainKeys
Active la vérification des messages entrants distants.

Vérifier les signatures DKIM
Active la vérification DKIM des messages entrants distants. Si vous avez activé la vérification des signatures DK et DKIM, et qu’un message contient ces deux types de signature ; la vérification DK n’est pas effectuée lorsque la signature DKIM indique que le message est valide. Si vous possédez SecurityPlus for MDaemon et que vous souhaitez utiliser le système de mises à jour urgentes 147 cette option doit obligatoirement être activée.

Résultats de la vérification

Si le message ne possède pas une signature valide requise :
Les options suivantes ne sont disponibles que si l’option ADSP est activée dans l’onglet Options DKIM 258. Si l’option ADSP n’est pas activée, les paramètres suivants n’auront aucun effet sur les messages.

...envoyer le code d’erreur 550
Lorsque l’enregistrement ADSP indique qu’une signature valide est requise, les messages qui n’en possèdent pas sont rejetés lors de la session SMTP et MDaemon renvoie le code d’erreur 550. Cependant, si la clé publique indique que l’utilisateur ne fait que tester DK/DKIM, le message est traité normalement.

...puis fermer la connexion
Cochez cette option si vous souhaitez que la connexion soit fermée immédiatement après l’envoi du code d’erreur 550 en cas de résultat "Fail" et de rejet du message. Si cette option est désactivée le message est rejeté mais la connexion reste ouverte.

...ajouter au score du Filtre anti-spam
Lorsque l’enregistrement ADSP indique qu’une signature valide est requise, le score de spam des messages qui n’en possèdent pas est modifié en conséquence. Cependant, si l’option *...envoyer le code d’erreur 550* ci-dessus

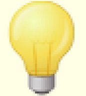
est activée, le message est rejeté. Dans tous les cas, si la clé publique indique que l'utilisateur ne fait que tester DK/DKIM, le message est traité normalement.



Cette option peut tout de même entraîner le rejet du message si le score de spam excède le seuil indiqué dans le Filtre anti-spam 209.

Si le message possède une signature et provient d'un domaine "accepté" :

...ajouter au score du Filtre anti-spam
Le score indiqué est attribué au message si le résultat de la vérification DK/DKIM est "Pass" et que le domaine expéditeur figure sur la liste des Domaines approuvés 264. Si le résultat de la vérification est "Pass", mais que le domaine ne figure pas parmi les domaines acceptés le score du Filtre anti-spam n'est pas modifié.



La valeur indiquée est généralement un nombre négatif afin que le score soit réduit pour les messages valides provenant d'un domaine accepté. Valeur par défaut : -0.5

Options de vérification

Ne pas vérifier les messsages provenant de sessions authentifiées
Les connexions authentifiées ne subissent pas de vérification cryptographique. Cela comprend les sessions vérifiées par Authentification SMTP 247, POP avant SMTP 245 ou le Bouclier IP 240.

Ne pas appliquer les vérifications cryptographiques aux connexions d'IP autorisées
Activez cette option si vous souhaitez que ces vérifications ne s'appliquent pas aux connexions provenant d'adresses IP autorisées.

Mettre en cache les résultats de la vérification
Cochez cette option si vous souhaitez mettre temporairement en cache les résultats des vérifications

Cache
Ouvre le fichier du cache de DK/DKIM.

Liste des exceptions
Ouvre la liste blanche ; ajoutez-y les adresses IP exemptes de vérification.

En-tête Authentication-Results

Lorsqu'un message est authentifié par SMTP AUTH, SPF, DomainKeys ou DKIM, MDaemon insère un en-tête dans le message contenant les résultats de l'authentification. Si la configuration de MDaemon permet la réception des messages dont l'authentification a échoué, l'en-tête contient un code qui précise les raisons de cet échec.



Des travaux sont en cours auprès de l'IETF (Internet Engineering Task Force) concernant cet en-tête et les protocoles d'authentification mentionnés ici. Plus d'informations sont disponibles à l'adresse: http://www.ietf.org/.

En-têtes DK/DKIM dans les messages de liste de diffusion

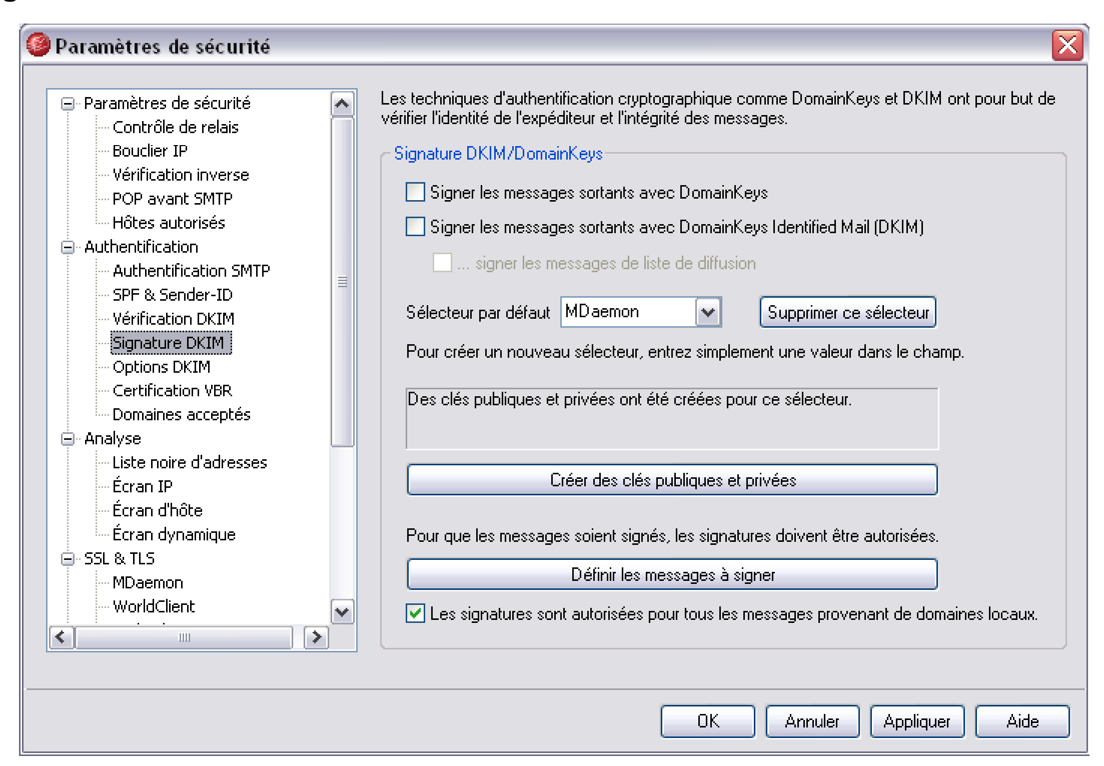
Par défaut, MDaemon supprime les signatures DK/DKIM des messages de liste entrants car elles risquent d'être corrompues lors du traitement de la liste. Si vous souhaitez tout de même laisser les signatures dans les messages de liste de diffusion, modifiez le fichier MDaemon.ini comme suit :

```
[DomainKeys]
StripSigsFromListMail=No (par défaut : Yes)
```

Voir également :

DomainKeys Identified Mail 251
Signature DKIM 255
Options DKIM 258

4.4.2.3.2 Signature DKIM



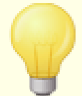
Cet onglet vous permet d'attribuer une signature aux messages sortants de votre choix. Il est également possible de désigner un sélecteur et de créer des clés publiques et privées correspondantes. Un sélecteur ("MDaemon"), une clé publique et privée par défaut sont créés automatiquement lors du démarrage de MDaemon. Ces clés sont uniques : elles ne se répètent jamais d'un site à l'autre, quel que soit le sélecteur. Par défaut, les clés sont créées avec une longueur de 1024 bits.

Signature DKIM/DomainKeys

Signer les messages sortants avec DomainKeys
Cochez cette option si vous souhaitez que MDaemon signe certains messages sortants. Seuls les messages correspondant à certains critères (définis en cliquant sur le bouton *Définir les messages à signer*) seront signés. De plus, ils doivent être destinés à une adresse distante et provenir d'une session authentifiée par SMTP AUTH. Les messages des listes de diffusion ne sont jamais signés. La signature des messages peut également être activée par une action du Filtre de contenu (*Sign with DKIM selector…*).

Signer les messages sortants avec DomainKeys Identified Mail (DKIM)
Cochez cette option si vous souhaitez que les messages sortants soient signés avec DKIM.

...signer les messages de liste de diffusion
Cochez cette option si vous souhaitez que tous les messages de liste de diffusion reçoivent une signature cryptographique. Dans ce cas, il n'est pas nécessaire de les ajouter aux messages à signer.



Pour signer du courrier de liste, chaque message doit être analysé par le Filtre de contenu, ce qui ralentit les performances du serveur pour les listes à fort trafic.

Sélecteur par défaut
Choisissez dans la liste déroulante le sélecteur dont les clés publiques/privées seront utilisées pour la signature des messages. Pour créer un nouveau sélecteur, saisissez son nom puis cliquez sur *Créer des clés publiques et privées*. Si vous souhaitez que certains messages soient signés avec un autre sélecteur, indiquez-le en cliquant sur *Définir les messages à signer* ou créez une règle du Filtre de contenu à l'aide de l'action *Sign with DomainKeys selector...*

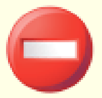
Supprimer ce sélecteur
Si vous souhaitez supprimer un sélecteur, cliquez sur ce bouton puis suivez les instructions à l'écran.

Créer des clés publiques et privées
Cliquez sur ce bouton pour créer la paire de clés correspondant au sélecteur défini ci-dessus. Lorsque les clés sont créées, le fichier dns_readme.txt est généré et s'ouvre automatiquement. Il contient des exemples de données que vous devez publier dans les enregistrements DNS contenant votre politique DomainKeys et la clé publique du sélecteur choisi. Ces exemples montrent comment indiquer s'il s'agit d'un test ou non, et si tous les messages doivent être signés, ou pas. Si vous souhaitez

tester DomainKeys ou un sélecteur, vous devrez utiliser les informations contenues dans les entrées "Testing" pour la politique ou le sélecteur, selon ce que vous désirez tester. Dans le cas contraire, utilisez les entrées "Not testing".

Toutes les clés sont enregistrées au format PEM. Les clés et les sélecteurs sont sauvegardés dans le dossier `\MDaemon\Pem` de la façon suivante :

```
\MDaemon\Pem\<Selector>\rsa.public - clé publique du sélecteur
\MDaemon\Pem\<Selector>\rsa.private - clé privée du sélecteur
```



Les fichiers contenus dans ces dossiers ne sont ni cryptés, ni masqués, mais ils contiennent les clés privées de cryptage RSA et ne doivent jamais être consultés par des personnes non autorisées. Il est recommandé d'en protéger l'accès à l'aide des paramètres de sécurité des dossiers du système d'exploitation.

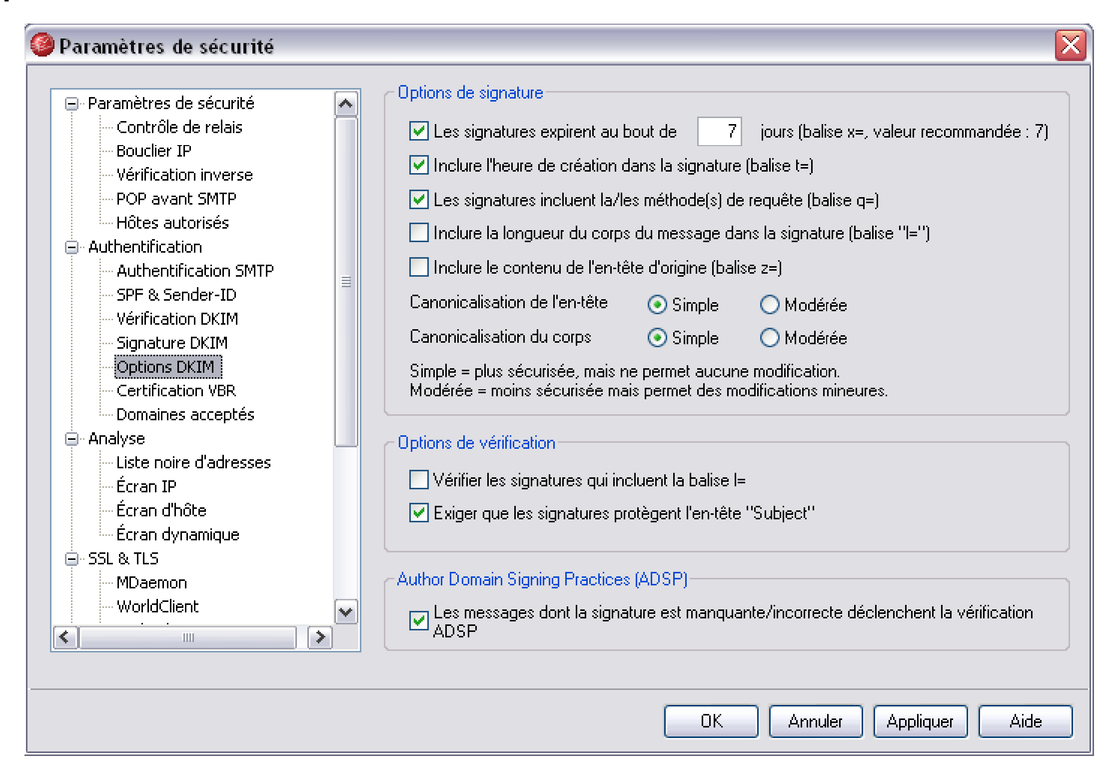
Définir les messages à signer
Après avoir coché l'une des options *Signer les messages sortants*, cliquez sur ce bouton afin de modifier le fichier `DKSign.dat`, qui contient la liste des domaines et adresses qui comporteront une signature. Vous devez aussi préciser pour chaque adresse si les messages devant être signés sont ceux qui en proviennent ou bien ceux qui lui sont adressés ; ou bien définir la signature en fonction d'en-têtes spécifiques tels que "`Reply-To`" ou "`Sender`". Vous avez également la possibilité de définir un sélecteur pour chaque entrée, qui sera utilisé pour signer les messages correspondant à cette entrée. Enfin, vous pouvez préciser le domaine à utiliser dans la balise "d=" tag de la signature. Cela peut être utile sous possédez plusieurs sous-domaines signant les messages. Dans ce cas, vous pouvez utiliser la balise "d=" pour indiquer aux serveurs destinataires que la clé DK/DKIM se trouve dans les enregistrements DNS d'un seul domaine. Les caractères joker sont autorisés dans les noms de domaines et les adresses.

Les signatures sont autorisées pour tous les messages provenant de domaines locaux
Utilisez cette option si vous souhaitez que tous les messages de vos domaines locaux fassent partie des messages à signer. Dans ce cas, il n'est pas nécessaire d'ajouter ces domaines à la liste des domaines à signer (dans le fichier DKSign.dat) sauf si vous souhaitez utiliser un sélecteur ou une balise "d=" spécifiques pour certains domaines. Cette option est activée par défaut.

Voir également :

DomainKeys Identified Mail 251
Options DKIM 258
Vérification DKIM 252

4.4.2.3.3 Options DKIM



Options de signature

Les signatures expirent au bout de X jours
Cochez cette option si vous souhaitez appliquer une limite de validité aux signatures et indiquez le nombre de jours souhaité. Les messages possédant une signature expirée ne seront pas reconnus par la vérification. Cette option correspond à la balise “x=” des signatures. Sa valeur par défaut est de 7 jours.

Inclure l'heure de création dans la signature (balise "t=")
Cochez cette case pour inclure la balise indiquant l'heure de création (balise "t=") dans la signature.

Les signatures incluent la/les méthodes de requête (balise "q=")
Cochez cette case pour inclure la balise indiquant la méthode de requête dans la signature DKIM (par ex. : q=dns).

Inclure la longueur du corps du message dans la signature (balise "l=")
Cochez cette case si vous souhaitez inclure la balise indiquant la longueur du corps du message dans les signatures DKIM.

Inclure le contenu de l’en-tête d’origine (balise z=)
Cochez cette case si vous souhaitez inclure la balise "z=" dans la signature DKIM. Cette balise contient une copie des en-têtes d’origine du message. Cela risque de rendre la signature assez volumineuse.

Canonicalisation

La canonicalisation est un procédé consistant à convertir les en-têtes et le corps d'un message et à les "normaliser" avant d'ajouter la signature DKIM. Cette opération est nécessaire car certains serveurs de messagerie et systèmes de relais apportent lors du traitement des modifications mineures aux messages qui risqueraient "d'endommager" les signatures si les messages n'étaient pas préparés avec un standard canonique. Il existe actuellement deux méthodes de canonicalisation pour les signatures DKIM : simple et modérée. La méthode simple est la plus stricte car elle n'autorise quasiment aucune modification du message. La méthode modérée autorise quelques modifications mineures.

Canonicalisation de l'en-tête : Simple / Modérée
Méthode de canonicalisation des en-têtes des messages. La méthode simple n'autorise aucune modification. La méthode modérée permet de convertir les noms des en-têtes (mais pas les valeurs) en minuscules, de remplacer plusieurs espaces par un seul, et d'autres modifications mineures.Paramètre par défaut : Simple.

Canonicalisation du corps : Simple / Modérée
Méthode de canonicalisation du corps des messages. La méthode simple ignore les lignes vides à la fin du corps (il s'agit de la seule modification autorisée). La méthode modérée autorise les lignes vides à la fin du message, ignore les espaces à la fin des lignes, remplace plusieurs espaces par un seul, etc. Paramètre par défaut : Simple.

Options de vérification

Vérifier les signatures qui incluent la balise "l"
Lorsque cette option est activée, MDaemon tient compte de la balise "l" lorsqu'elle est incluse dans la signature DKIM d'un message entrant. Si la longueur du corps du message est plus importante que la valeur de cette balise, MDaemon ne vérifie que la valeur indiquée dans la balise (le reste du message n'est pas vérifié). Cela signifie que des données (pouvant être suspectes) ont été ajoutées au message. Si la longueur du corps est inférieure à la valeur de la balise, la vérification de la signature échoue (résultat : FAIL), car cela signifie qu'une partie du message a été supprimée.

Exiger que les signatures protègent l'en-tête Subject
Activez cette option si vous souhaitez exiger que la signature DKIM des messages entrants protège l'en-tête Subject.

Author Domain Signing Practices (ADSP)

Les messages dont la signature est manquante ou incorrecte déclenchent la vérification ADSP
Activez cette option si vous souhaitez appliquer les enregistrements ADSP lorsque la signature d'un message entrant est manquante ou incorrecte. Si cette option est désactivée ou si l'enregistrement SSP utilise une syntaxe ultérieure, MDaemon considère que le domaine expéditeur ne signe qu'une partie de ses messages et le message est considéré comme "non suspect".

Voir également :

[DomainKeys Identified Mail](251)
[Vérification DKIM](252)
[Signature DKIM](255)

4.4.2.4 Certification des messages

La certification des messages est un procédé par lequel des fournisseurs de services de certification se "portent garants" de la bonne conduite de l'expéditeur d'un message. Par conséquent, les messages envoyés depuis un domaine pour lequel un fournisseur de certification se porte garant peuvent être plus facilement considérés comme légitimes. La certification permet d'éviter que des messages soient soumis inutilement au Filtre anti-spam et diminue les ressources nécessaires pour le traitement de chaque message.

MDaemon Pro supporte la certification des messages et inclut la première application commerciale d'un protocole appelé VBR (Vouch-By-Reference). De par sa participation au Domain Assurance Council (www.domain-assurance.org) Alt-N Technologies contribue à la création et à l'extension de ce protocole. VBR fournit le mécanisme par lequel des fournisseurs de services de certification se portent garants pour des domaines.

Certification des messages entrants

La vérification de la certification des messages entrants est simple à configurer. Il suffit de cocher l'option *Activer la certification pour les messages entrants* (Sécurité » Paramètres de sécurité » Certification VBR) et d'indiquer un ou plusieurs services à utiliser pour vérifier les messages entrants. Il est également possible de ne pas soumettre les messages ainsi vérifiés au Filtre anti-spam ou d'ajuster leur score de spam en conséquence.

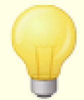
Certification des messages sortants

Avant de configurer la certification des messages sortants dans MDaemon, vous devez posséder un fournisseur de services de certification pour vos messages. Alt-N Technologies fournit un service de certification VBR aux utilisateurs de MDaemon. Pour en savoir plus, consultez : www.altn.com.

Une fois que vous avez souscrit les services d'un fournisseur pour vos messages :

1. Cliquez sur Sécurité » Paramètres de sécurité » Certification VBR.
2. Activez l'option *Insérer des données de certification dans les messages sortants.*
3. Cliquez sur le bouton *Configurer la certification des messages pour un domaine*.
4. Indiquez dans la fenêtre qui s'ouvre ensuite un *Nom de domaine*.
5. Indiquez dans le menu déroulant *Type de messages* les messages que votre fournisseur de services accepte de certifier ou saisissez un type s'il ne figure pas dans la liste.

6. Indiquez le nom d'hôte du service de certification de vos messages sortants. Si vous en possédez plusieurs, séparez-les par des espaces.
7. Cliquez sur *OK*.
8. Configurez MDaemon pour qu'il signe les messages sortants avec DKIM ou DK 251, ou bien activez les options SPF ou SIDF 249. Cela permet de garantir l'identité de l'expéditeur du message. Un message ne peut pas être certifié si le serveur destinataire ne peut pas vérifier s'il est authentique.



Avec le protocole VBR, les messages ne sont pas transmis au fournisseur de services de certification, ni signées par lui. Il se porte simplement "garant de la bonne conduite" du domaine pour l'envoi de messages.

Pour en savoir plus sur les services de certification fournis par Alt-N Technologies, consultez :

http://www.altn.com/email-certification/

Pour en savoir plus sur le protocole VBR et la certification des messages, consultez :

http://www.domain-assurance.org/

Spécification VBR—Internet-Draft 00 :

http://files.altn.com/MDaemon/drafts/draft-hoffman-dac-vbr-00.txt

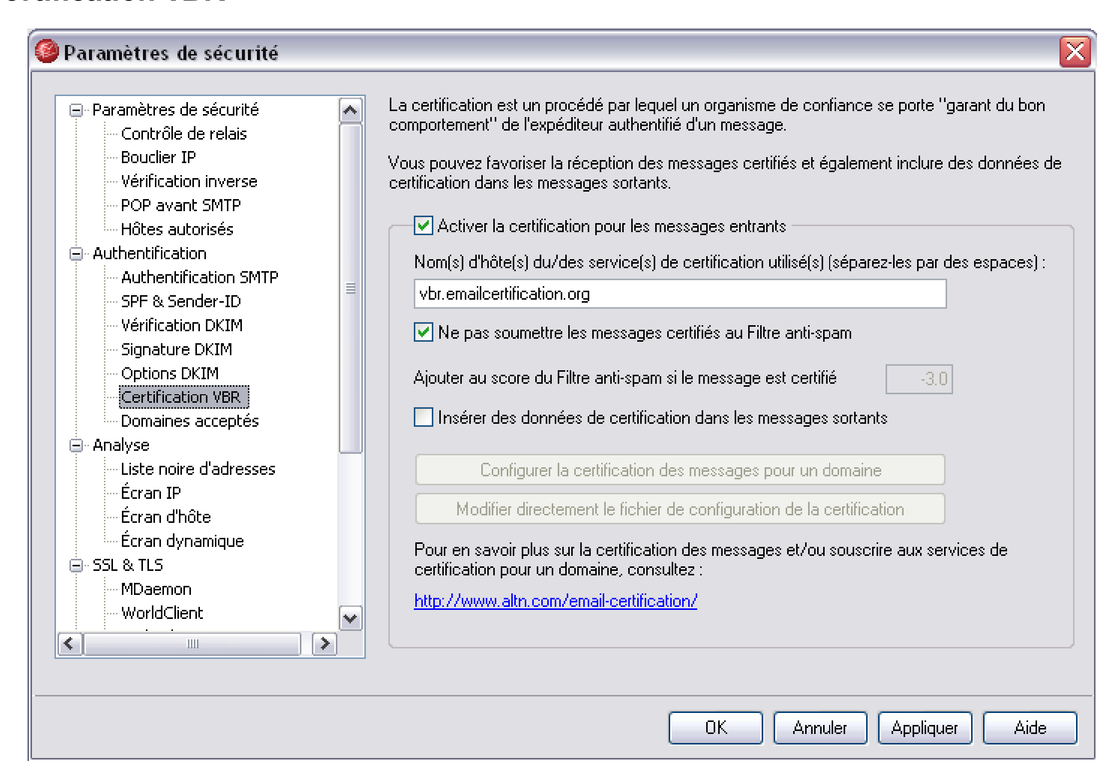
For more information on DKIM visit:

http://www.dkim.org/

Voir également :

Certification VBR 262

4.4.2.4.1 Certification VBR



Pour accéder à cette boîte de dialogue, cliquez sur : Sécurité » Paramètres de sécurité » Authentification » Certification VBR.

Certification des messages

Activer la certification pour les messages entrants
Lorsque cette option est activée, MDaemon vérifie la certification des messages reçus. Si le message est correctement "certifié", il est possible de ne pas le soumettre au Filtre anti-spam ou bien d'ajuster son Score de spam 208.

Nom(s) d'hôte(s) du/des service(s) de certification utilisés(s) (séparez-les par des espaces) :
Indiquez le nom du service de certification que vous souhaitez utiliser pour vérifier les messages reçus. Si vous en possédez plusieurs, séparez-les par des espaces.

Ne pas soumettre les messages certifiés au Filtre anti-spam
Activez cette option si vous souhaitez que le Filtre anti-spam ne s'applique pas aux messages certifiés.

Ajouter au score du Filtre anti-spam si le message est certifié
Si vous souhaitez tout de même soumettre les messages certifiés au Filtre anti-spam, il est possible d'ajuster leur score de spam. Pour que cette option ait un effet "bénéfique" sur le score, le nombre doit être négatif (par défaut : -3.0.).

Insérer des données de certification dans les messages sortants
Activez cette option si vous souhaitez certifier vos messages sortants. Cliquez

ensuite sur le bouton *Configurer la certification des messages pour un domaine*.

Configurer la certification des messages pour un domaine
Ce bouton ouvre une fenêtre dans laquelle vous devez indiquer le domaine pour lequel les messages sont certifiés, le type de messages ainsi que le fournisseur de services de certification.

Modifier directement le fichier de configuration de la certification
Tous les domaines déjà configurés figurent dans ce fichier. Il est donc possible de modifier manuellement son contenu ou bien d'ajouter d'autres entrées.

Paramètres de certification



Cette fenêtre s'affiche lorsque l'on clique sur le bouton *Configurer la certification des messages* pour un domaine.

Nom de domaine
Indiquez le nom du domaine pour lequel les messages sortants doivent être certifiés.

Rechercher
Si vous avez déjà configuré la certification pour un domaine, indiquez son nom dans le champ ci-dessus et cliquez sur ce bouton. Les paramètres de ce domaine s'affichent alors.

Type de messages
Indiquez dans ce menu déroulant les messages que votre fournisseur de services

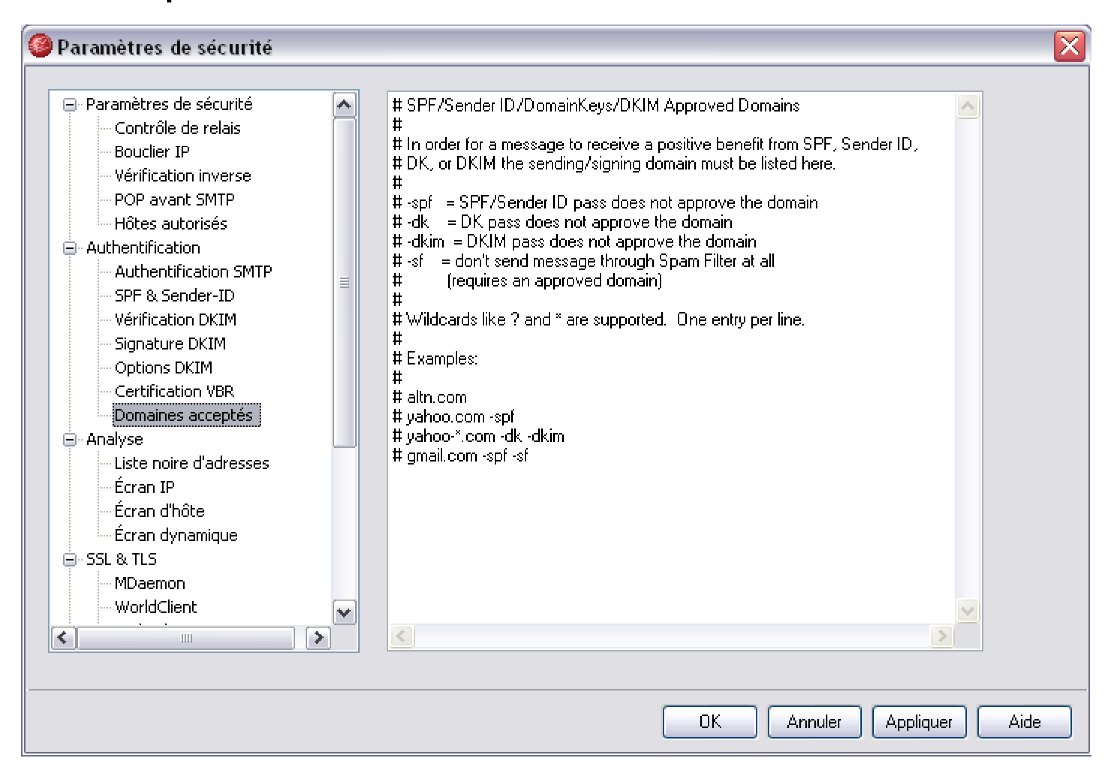
accepte de certifier ou saisissez un type s'il ne figure pas dans la liste.

Nom d'hôte du/des services...
Indiquez le nom d'hôte du service de certification de vos messages sortants (par exemple vbr.emailcertification.org). Si vous en possédez plusieurs, séparez-les par des espaces.

Voir également :

Certification des messages 260

4.4.2.5 Domaines acceptés



Certains spammeurs utilisent à présent SPF ou intègrent des signatures DK/DKIM valides dans leurs messages. Par conséquent, une signature valide ne garantit pas toujours que le message n'est pas du spam. C'est pourquoi une signature SPF, Sender ID, DK, ou DKIM valide ne baisse le score de spam attribué au message que si le domaine dont il provient figure sur la liste des domaines acceptés. Cette liste fonctionne de façon similaire à une liste blanche : ajoutez les domaines pour lesquels vous souhaitez baisser le score de spam lorsqu'une vérification cryptographique est réussie.

Lorsqu'un message signé par l'un de ces domaines est vérifié avec succès par SPF, Sender ID, DK ou DKIM, son score de façon sera réduit en fonction des paramètres définis dans les onglets SPF & Sender ID 249 et Vérification DKIM 252. Vous pouvez

toutefois utiliser les balises ci-dessous lors de l'ajout d'un domaine à la liste :

-spf ne pas baisser le score de spam des messages de ce domaine, même si la vérification SPF ou Sender ID est valide.

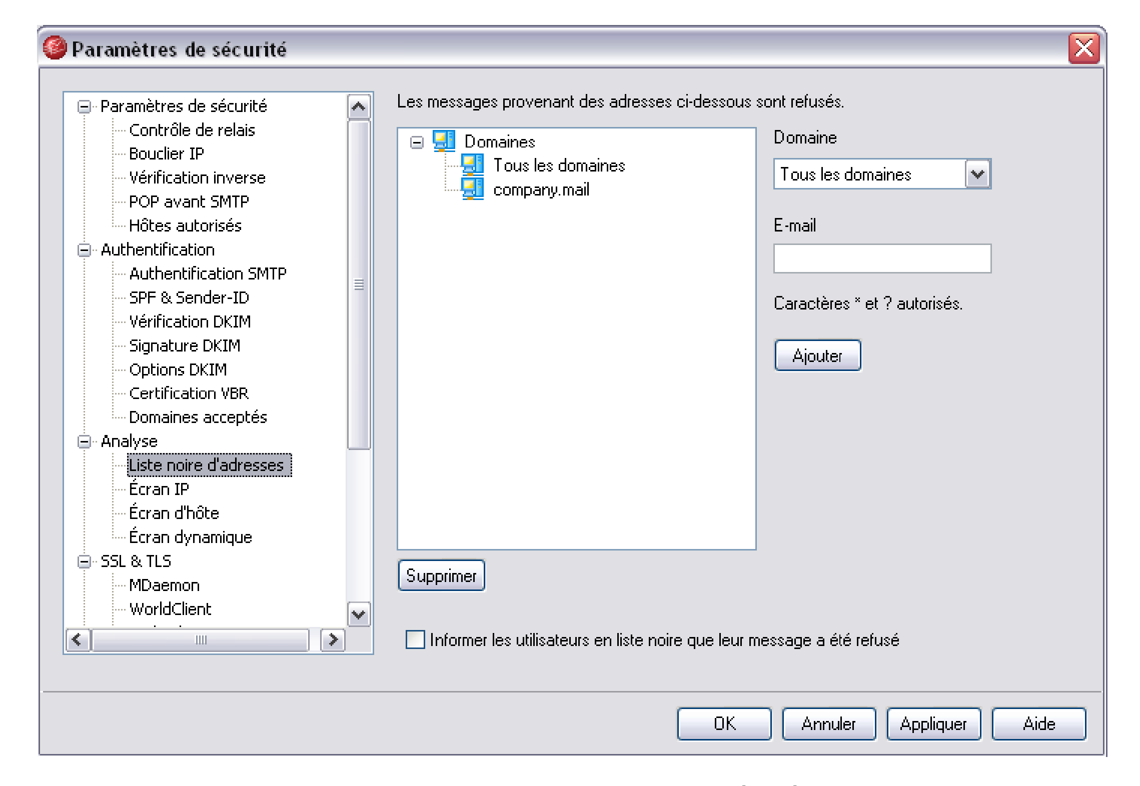
-dk ne pas baisser le score de spam des messages de ce domaine, même si la vérification DK est valide.

-dkim ne pas baisser le score de spam des messages de ce domaine, même si la vérification DKIM est valide.

-sf ne pas soumettre au Filtre anti-spam les messages du domaine dont la vérification est valide.

4.4.3 Analyse

4.4.3.1 Liste noire d'adresses



Cette liste contient les adresses qui ne sont pas autorisées à envoyer du courrier sur votre serveur. Si un message envoyé par une adresse de la liste arrive sur le serveur, il est refusé durant la session SMTP. Cette fonctionnalité permet de contrôler les utilisateurs qui posent problème. Les adresses se configurent par domaine ou de manière globale (c'est-à-dire pour tous les domaines MDaemon).

Les messages provenant des adresses ci-dessous sont refusés
Cette fenêtre contient les adresses actuellement interdites, répertoriées par domaine.

Domaine
Sélectionnez un domaine pour lequel cette adresse est interdite (domaine qui ne pourra pas recevoir de courrier de cette adresse interdite). Sélectionnez "All Domains" pour interdire l'adresse de manière globale.

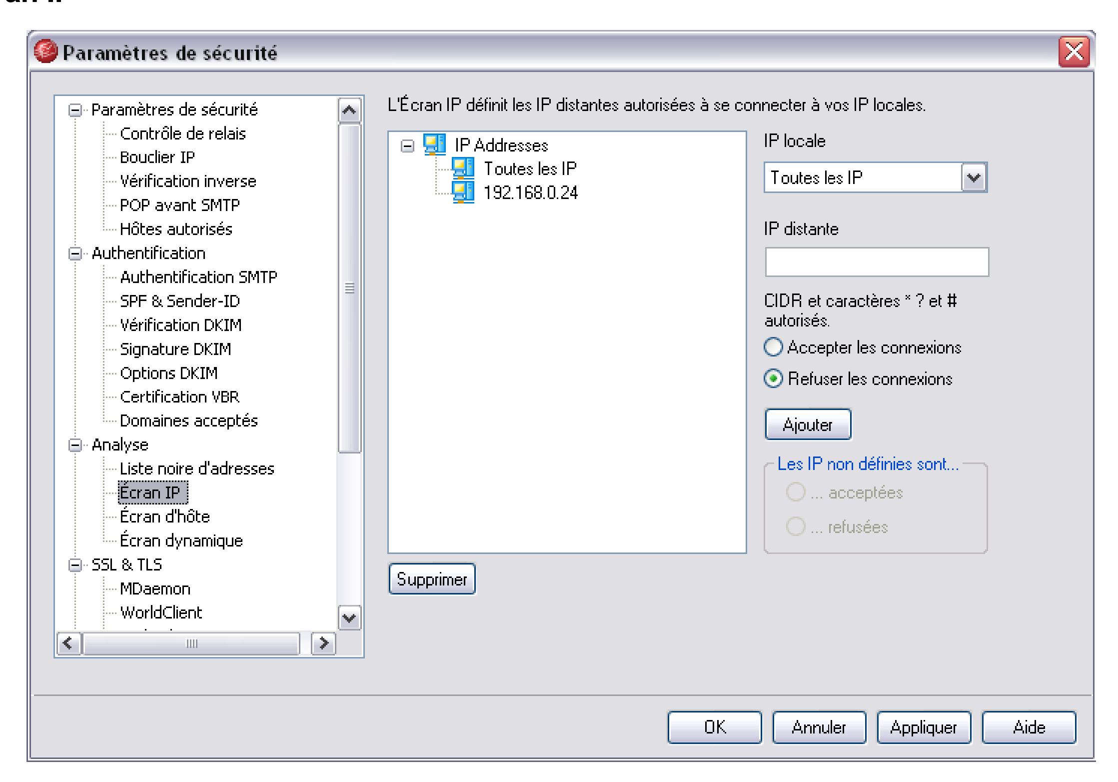
E-mail
Saisissez les adresses que vous souhaitez interdire. Les caractères jokers sont autorisés : "*@badmail.com" interdit les messages envoyés par les utilisateurs de "badmail.com", et "frank@*" interdit les messages envoyés par les utilisateurs prénommés “frank”, quel que soit le domaine d'envoi du message.

Ajouter
Cliquez sur ce bouton pour ajouter l'adresse saisie à la liste.

Supprimer
Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur ce bouton.

Informer les utilisateurs en liste noire que leur message a été refusé
Lorsque cette option est activée, l'expéditeur dont l'adresse est interdite reçoit un message lui notifiant la suppression de son courrier.

4.4.3.2 Écran IP



L'Écran IP se trouve dans : Sécurité » Paramètres de sécurité » Analyse. L'écran IP est la liste des adresses IP distantes autorisées à se connecter à vos adresses IP

locales. Vous pouvez indiquer une liste d'adresses IP, puis configurer le serveur pour qu'il n'autorise que les connexions depuis les adresses figurant dans cette liste, ou pour qu'il refuse toutes les tentatives de connexion depuis une adresse IP figurant sur cette liste. Les adresses indiquées dans l'Écran IP peuvent être associées à une IP locale spécifique ou toutes les IP locales. La notation CIDR et les caractères joker *, #, et ? sont autorisés. Exemples :

..*.*	Correspond à n'importe quelle adresse IP
#.#.#.#	Correspond à n'importe quelle adresse IP
192.*.*.*	Correspond à toutes les adresses IP commençant par 192
192.168.*.239	Correspond à toutes les adresses IP comprises entre 192.168.0.239 et 192.168.255.239
192.168.0.1??	Correspond à toutes les adresses IP comprises entre 192.168.0.100 et 192.168.0.199

IP locale
Sélectionnez dans la liste déroulante soit "All IPs" (toutes les IP), soit l'IP locale à laquelle vous souhaitez que l'Écran IP s'applique.

IP distante
Entrez l'adresse IP que vous souhaitez ajouter à la liste.

Accepter les connexions
En sélectionnant cette option, les adresses IP indiquées sous le domaine donné pourront se connecter et envoyer du courrier.

Refuser les connexions
En sélectionnant cette option, les tentatives de connexion depuis des adresses IP indiquées dans cette liste d'adresses seront refusées et immédiatement annulées.

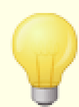
Ajouter
Après avoir configuré les options ci-dessus, cliquez sur ce bouton pour ajouter une adresse à la liste.

Supprimer
Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur ce bouton.

Les IP non définies sont...

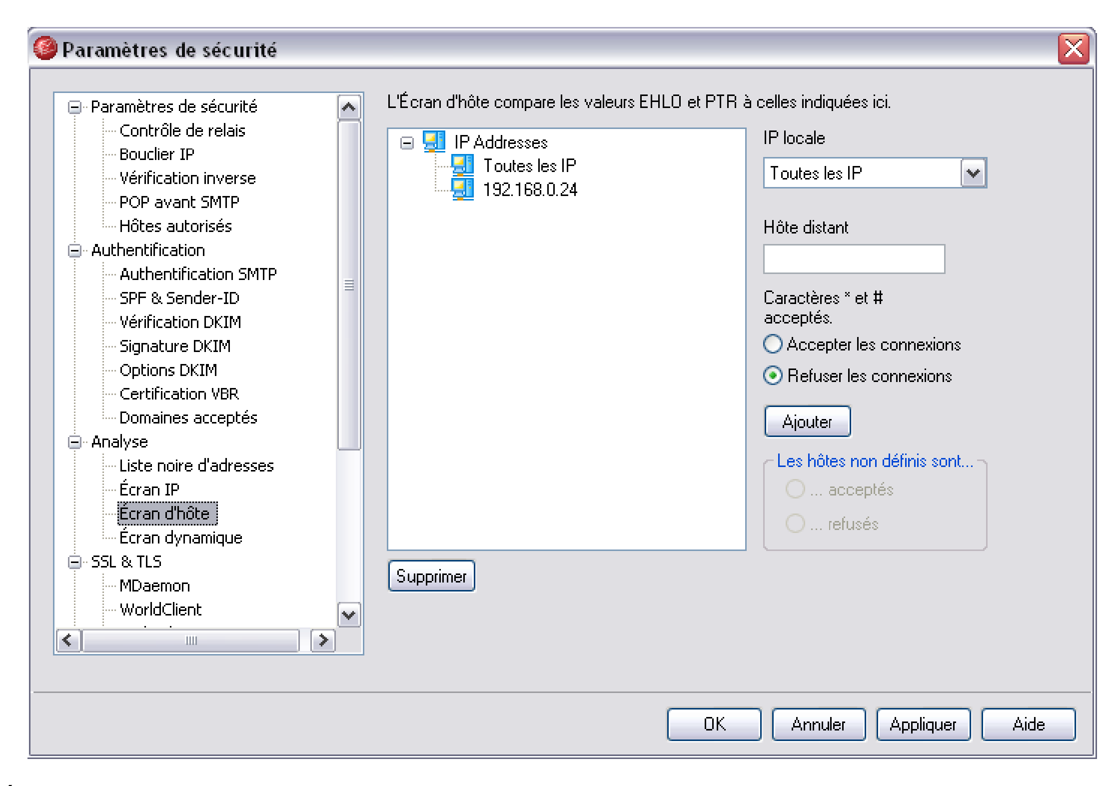
...acceptées
Lorsque cette option est activée, toutes les adresses IP qui ne sont pas répertoriées dans l'écran IP pourront se connecter.

...refusées
Lorsque cette option est activée, seules les adresses IP autorisées inscrites dans l'écran IP pourront se connecter.



L'Écran IP ne bloque jamais les IP locales ou autorisées 246.

4.4.3.3 Écran d'hôte



L'Écran d'hôte se trouve dans : Sécurité » Paramètres de sécurité » Analyse. Il contient est la liste des hôtes distantes autorisés à se connecter à vos adresses IP locales. Vous pouvez indiquer une liste d'hôtes, puis configurer le serveur pour qu'il n'autorise que les connexions depuis les adresses figurant dans cette liste, ou pour qu'il refuse toutes les tentatives de connexion depuis ces hôtes. Pour cela, il compare les valeurs EHLO et PTR transmises durant la session SMTP aux valeurs indiquées ici.

IP locale
Sélectionnez dans la liste déroulante soit "All IPs" (toutes les IP), soit l'IP locale à laquelle vous souhaitez que l'Écran d'hôte s'applique.

Hôte distant
Entrez l'hôte que vous souhaitez ajouter à la liste.

Accepter les connexions
En sélectionnant cette option, les hôtes indiqués sous le domaine donné pourront se connecter et envoyer du courrier.

Refuser les connexions
En sélectionnant cette option, les tentatives de connexion depuis des hôtes indiqués dans cette liste d'adresses seront refusées et immédiatement annulées.

Ajouter
Après avoir configuré les options ci-dessus, cliquez sur ce bouton pour ajouter un hôte à la liste.

Supprimer
Pour supprimer un hôte de la liste, sélectionnez-le et cliquez sur ce bouton.

Les hôtes non définis sont...

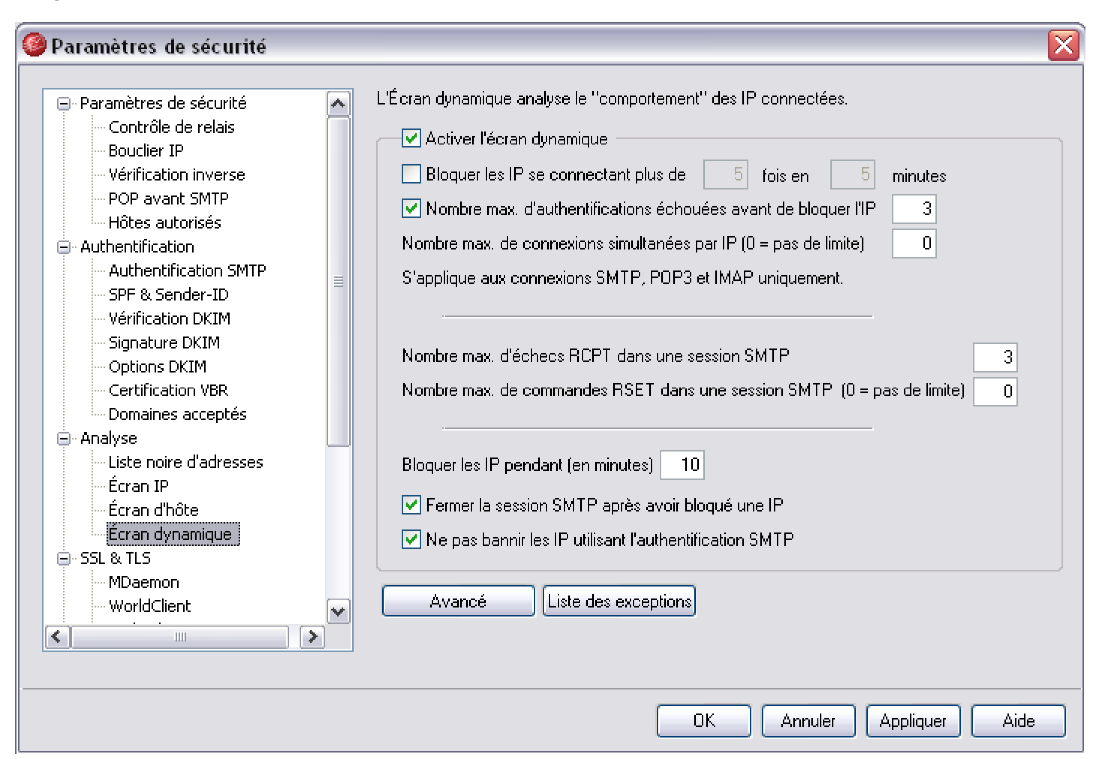
...acceptés
Lorsque cette option est activée, tous les hôtes qui ne sont pas répertoriés dans l'Écran d'hôte pourront se connecter.

...refusés
Lorsque cette option est activée, seuls les hôtes inscrits dans l'Écran d'hôte pourront se connecter.



L'Écran d'hôte ne bloque jamais les IP locales ou autorisées 246.

4.4.3.4 Écran dynamique



Avec l'Écran dynamique, MDaemon analyse le "comportement" des serveurs lui envoyant du courrier. Par exemple, il est possible de refuser temporairement les

connexions d'une adresse IP si le nombre d'erreurs "destinataire inconnu" au cours de la session est trop important. De même, vous pouvez bloquer les IP qui se connectent trop souvent à votre serveur au cours d'une période définie, ainsi que celles dont l'authentification échoue un nombre de fois supérieur à celui indiqué.

Lorsqu'une adresse est bloquée, cette mesure n'est pas permanente : elle s'applique pendant le nombre de minutes choisi. Le bouton *Avancé* ouvre le fichier DynamicScreen.dat, contenant la liste des IP bloquées ainsi que la durée appliquée pour chacune d'entre elles. Ce fichier reste en mémoire et peut être modifié en cliquant sur *Avancé* ou en l'ouvrant avec un éditeur de texte. Remarque : si vous le modifiez manuellement, créez ensuite un fichier vide appelé TARPIT.SEM dans le répertoire \APP\ de MDaemon. Ainsi, le fichier DynamicScreen.dat est actualisé et les modifications sont aussitôt prises en compte.

Écran dynamique

Activer l'Écran dynamique
Cochez cette case pour activer l'Écran dynamique.

Bloquer les IP se connectant plus de [X] fois en [X] minutes
Cochez cette case pour bloquer les tentatives intempestives de connexion sur votre serveur.

Nombre max. d'authentifications échouées avant de bloquer l'IP
Correspond au nombre de tentatives d'authentification échouées au bout duquel l'IP connectée est bannie. Cela évite que des comptes ne soient "piratés" et utilisés à mauvais escient. Cette option s'applique aux connexions SMTP, POP3 et IMAP.

Nombre max. de connexions simultanées par IP (0 = pas de limite)
Correspond au nombre maximum autorisé de connexions simultanées provenant de la même IP avant que l'IP ne soit bannie. Indiquez "0" si vous ne souhaitez pas imposer de limite.

Nombre maximum d'échecs RCPT dans une session SMTP
Correspond au nombre d'erreurs "destinataire inconnu" (pendant une même session) au bout duquel l'adresse IP est bloquée. Lorsque cette erreur se produit fréquemment, cela signifie généralement que l'expéditeur est un spammeur, car les spammeurs utilisent pour la plupart des adresses invalides.

Nombre max. de commandes RSET dans une session SMTP (0 = pas de limite)
Utilisez cette option si vous souhaitez bloquer les adresses IP envoyant trop de commandes RSET. Indiquez "0" si vous ne souhaitez pas imposer de limite. L'onglet Serveurs38 du domaine par défaut contient une option globale similaire.

Bloquer les IP pendant (en minutes)
Indiquez la période pendant laquelle les IP bannies par l'une des options ci-dessus ne pourront se connecter à votre serveur. Une fois ce délai écoulé, elles pourront à nouveau vous envoyer du courrier normalement. Cela permet d'éviter de bloquer de façon permanente un expéditeur valide banni accidentellement.

Fermer la session SMTP après avoir bloqué une IP
Activez cette option pour fermer la session SMTP lorsqu'une IP est bloquée par l'une des options ci-dessus.

Ne pas bannir les IP utilisant l'authentification SMTP
Cochez cette case pour ne pas appliquer l'Écran dynamique aux sessions authentifiées.

Avancé
Ouvre le fichier DynamicScreen.dat, contenant la liste de toutes les adresses IP actuellement rejetées par l'Écran dynamique. Il est possible d'ajouter manuellement des adresses sous la forme : Adresse<espace>Minutes. Par exemple : 192.168.0.1 60, signifie que cette adresse sera bloquée pendant 60 minutes.

Liste des exceptions
Cliquez sur ce bouton pour afficher la liste blanche du système de répulsion et de l'Écran dynamique. Les adresses figurant sur cette liste ne seront pas soumises au système de répulsion, ni à l'Écran dynamique.

4.4.4 SSL & TLS

MDaemon supporte le protocole SSL (Secure Sockets Layer)/TLS (Transport Layer Security) pour SMTP, POP, IMAP, WebAdmin et WorldClient. Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard qui permet de sécuriser les communications Internet entre le serveur et le client. Ce protocole fournit l'authentification du serveur, le cryptage des données et l'authentification facultative du client pour une connexion TCP/IP. De plus, dans la mesure où SSL est intégré aux principaux navigateurs actuels, vous n'avez qu'à installer un certificat valide sur votre serveur pour que les fonctions SSL de votre navigateur soient activées lors de la connexion avec WorldClient.

Si vous vous connectez aux ports de messagerie standard via un client de messagerie au lieu d'utiliser WorldClient, MDaemon peut donner la priorité à l'extension STARTTLS sur TLS pour SMTP et IMAP, et à l'extension STLS pour POP3. Toutefois, votre client doit d'abord être configuré pour utiliser SSL et doit prendre en charge ces extensions.

Enfin, vous pouvez aussi désigner des ports spécifiques pour les connexions SSL. Cette démarche n'est pas indispensable mais elle offre un meilleur accès aux clients qui ne sont pas compatibles avec certaines extensions SSL.

Les options permettant d'activer et de configurer le protocole SSL se trouvent dans : Sécurité » Paramètres de sécurité » SSL & TLS. Le ports SSL pour SMTP, POP3 et IMAP se trouvent dans l'onglet Ports41 dans : Configuration » Domaine/Serveurs par défaut.

Pour obtenir des informations sur la création et l'utilisation de certificats SSL, voir :

Création & utilisation de serveurs SSL281

—

Le protocole TLS/SSL est défini dans la RFC 2246, disponible à l'adresse :

http://www.rfc-editor.org/rfc/rfc2246.txt

L'extension STARTTLS pour SMTP est définie dans la RFC 3207 disponible à l'adresse :

http://www.rfc-editor.org/rfc/rfc3207.txt

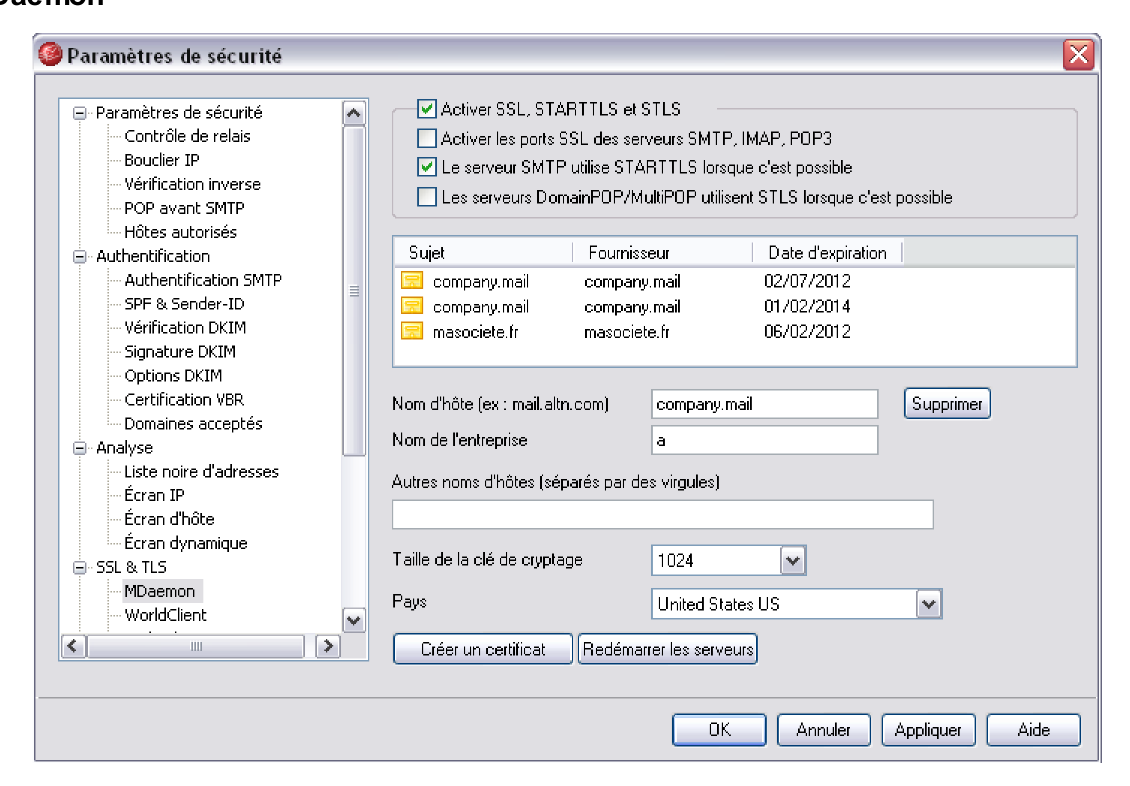
L'utilisation de TLS avec les protocoles IMAP et POP3 est définie dans la RFC 2595 disponible à l'adresse :

http://www.rfc-editor.org/rfc/rfc2595.txt

Voir également :

SSL & TLS » MDaemon 272
SSL & TLS » WorldClient 275
SSL & TLS » WebAdmin 278

4.4.4.1 MDaemon



Activer SSL, STARTTLS et STLS
Cochez cette case pour activer le support pour les protocoles SSL/TLS et les extensions STARTTLS et STLS. Choisissez ensuite le certificat que vous voulez utiliser.

Activer les ports SSL des serveurs SMTP, IMAP, POP3
Sélectionnez cette option si vous souhaitez activer les ports SSL dédiés spécifiés dans l'onglet Ports 41 du Domaine par défaut. Cette option ne s'applique pas aux clients qui utilisent STARTTLS et STLS sur les ports de messagerie par défaut (elle fournit simplement un support supplémentaire pour SSL).

Le serveur SMTP utilise STARTTLS lorsque c'est possible
Sélectionnez cette option si vous souhaitez que MDaemon essaie d'utiliser l'extension STARTTLS pour tous les envois de messages SMTP. Si MDaemon se connecte à un serveur qui ne supporte pas STARTTLS, le message sera alors envoyé normalement, sans utiliser SSL.

Les serveurs DomainPOP/MultiPOP utilisent STLS lorsque c'est possible
Cochez cette case si vous souhaitez que les serveurs DomainPOP et MultiPOP utilisent l'extension STLS lorsque c'est possible.

Liste des certificats

Cliquez une fois sur le certificat de la liste que le serveur de messagerie devra utiliser. Double-cliquez sur un certificat pour visualiser les détails le concernant dans la boîte de dialogue Certificat.



MDaemon ne permet pas à plusieurs domaines de posséder leur propre certificat. Tous les domaines de messagerie doivent donc partager un même certificat. Si vous avez plusieurs domaines, entrez leur nom dans le champ *Autres nom d'hôtes (séparés par des virgules)*, situé en dessous.

Supprimer
Sélectionnez un certificat dans la liste puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous voulez vraiment supprimer ce certificat.

Les commandes suivantes servent à créer un certificat. Pour en modifier un, double-cliquez le certificat souhaité dans la liste au-dessus.

Nom d'hôte
Saisissez le nom de l'hôte auquel vos utilisateurs se connecteront (par exemple, "courrier.exemple.com").

Nom de l'entreprise
Saisissez le nom de l'organisme ou de la société qui "détient" le certificat.

Autres noms d'hôtes (séparés par des virgules)
Actuellement, MDaemon ne permet pas à plusieurs domaines de posséder leur propre certificat : ils doivent donc tous partager le même. Saisissez dans ce champ, en les séparant par des virgules, le nom des autres domaines auxquels les utilisateurs se connecteront et auxquels le certificat s'appliquera. Les caractères jokers sont acceptés. Ainsi, "*.exemple.com" s'appliquera à tous les sous-domaines d'exemple.com (par exemple, "wc.exemple.com", "courrier.exemple.com", etc.).

Taille de la clé de cryptage
Choisissez la longueur, en bits, de la clé de cryptage pour ce certificat. Plus la clé cryptage est longue, plus le transfert des données est sécurisé. Veuillez noter que toutes les applications ne supportent pas toutes des clés de plus de 512 bits.

Pays
Indiquez dans quel pays se trouve votre serveur.

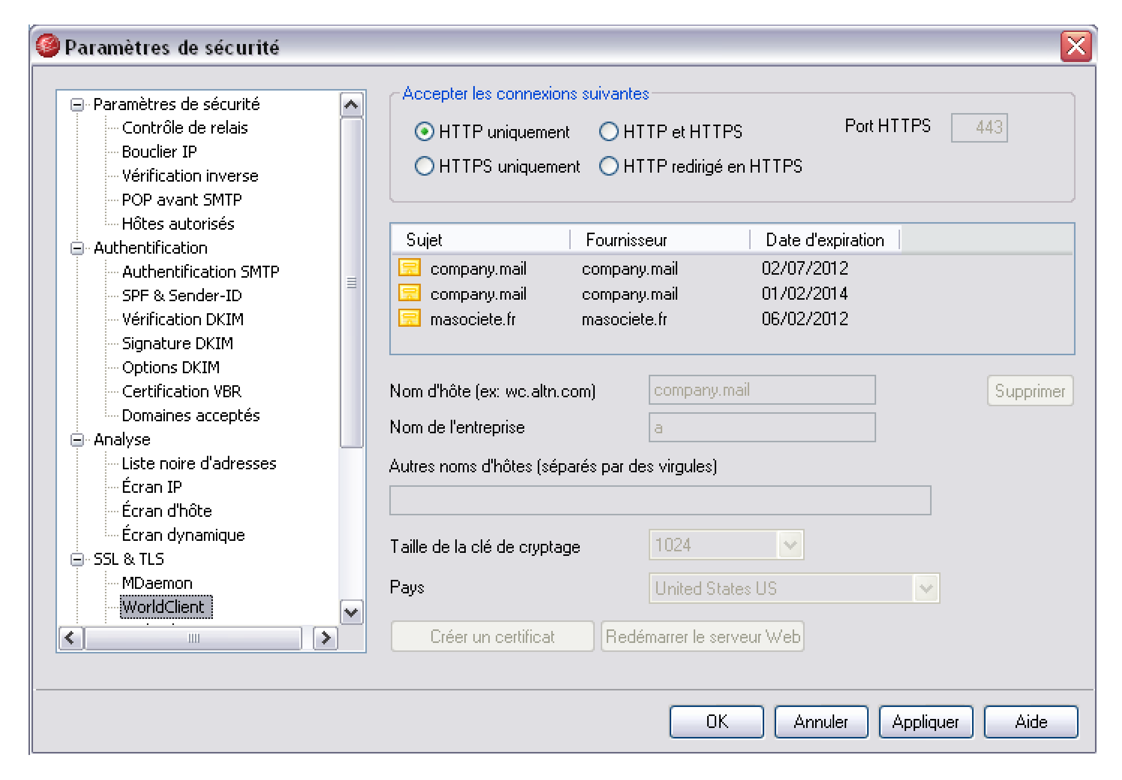
Créer un certificat
Lorsque vous avez saisi toutes les informations requises dans les commandes précédentes, cliquez sur ce bouton pour créer votre certificat.

Redémarrer les serveurs
Cliquez sur ce bouton pour redémarrer les serveurs SMTP/IMAP/POP. Ces derniers doivent être relancés après avoir modifié un certificat.

Voir également :

SSL & TLS 271
Création et utilisation de certificats SSL 281

4.4.4.2 WorldClient



Le serveur Web de MDaemon supporte le protocole SSL (Secure Sockets Layer). Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il fournit l'authentification du serveur, le cryptage de données, et l'authentification facultative du client pour la connexion TCP/IP. De plus, dans la mesure où SSL est intégré aux principaux navigateurs actuels, en installant simplement un certificat numérique valide sur votre serveur, les fonctions SSL du client qui se connecte sont activées.

Les options relatives à l'activation et à la configuration de WorldClient pour qu'il utilise le protocole SSL/HTTPS, se trouvent dans la boîte de dialogue SSL & HTTPS (Configuration » Services Web, synchro & MI » WorldClient". Pour plus de commodité, ces options sont également accessibles dans la boîte de dialogue "Configuration » Services web & SyncML » WorldClient".

Pour en savoir plus sur ce protocole, voir : **SSL & certificats** 271



Les éléments de cette boîte de dialogue s'appliquent uniquement lorsque WorldClient utilise le serveur web intégré de MDaemon. Si vous avez configuré WorldClient pour fonctionner un autre serveur, ces options ne seront alors pas utilisées—le support SSL/HTTPS doit être configuré dans le serveur choisi.

Accepter les connexions suivantes

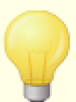
HTTP uniquement
Sélectionnez cette option si vous ne souhaitez pas autoriser les connexions HTTPS à WorldClient. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS
Cette option accepte le support SSL pour WorldClient, mais les utilisateurs ne sont pas obligés d'employer des connexions HTTPS. Dans ce cas WorldClient écoute les connexions HTTPS sur le port indiqué dans l'onglet Serveur web 111 des paramètres de WorldClient, mais il répond également aux connexions HTTP normales.

HTTPS uniquement
Avec cette option, il est obligatoire d'utiliser une connexion HTTPS pour se connecter à WorldClient. Les requêtes HTTP ne sont pas acceptées.

HTTP redirigé en HTTPS
Sélectionnez cette option pour rediriger toutes les connexions HTTP sur le port HTTPS.

Port HTTPS
Il s'agit du port TCP que WorldClient écoutera pour les connexions SSL. Le port SSL par défaut est le port 443. Si le port SSL par défaut est utilisé, vous n'aurez pas à inclure le numéro du port dans l'URL de WorldClient lors de la connexion par HTTPS (https://exemple.com est équivalent à https://exemple.com:443).



Le port HTTPS n'est pas le même que celui indiqué dans l'onglet Serveur Web 111 des propriétés de WorldClient. Si vous autorisez toujours les connexions HTTP vers WorldClient, ces connexions devront alors utiliser cet autre port pour pouvoir être effectuées correctement. Les connexions HTTPS doivent utiliser le port HTTPS.

Certificats

Cette boîte présente vos certificats SSL. Cliquez une fois sur un certificat pour le sélectionner et l'utiliser. Double-cliquez sur un certificat pour visualiser les détails le concernant dans la boîte de dialogue Certificat.



MDaemon ne permet pas à WorldClient d'utiliser plusieurs certificats. Tous les domaines de WorldClient doivent donc partager un même certificat. Si vous avez plusieurs domaines WorldClient, entrez leur nom (et celui des autres domaines auxquels vous souhaitez autoriser l'accès à WorldClient) dans le champ *Autres noms d'hôtes*, situé en dessous.

Supprimer
Sélectionnez un certificat dans la liste puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous voulez vraiment

supprimer ce certificat.

Nom d'hôte
Saisissez le nom de l'hôte auquel vos utilisateurs se connecteront (par exemple, « courrier.exemple.com »).

Nom de l'entreprise
Saisissez le nom de l'organisme ou de la société "propriétaire" du certificat.

Autres noms d'hôtes (séparés par des virgules)
Actuellement, MDaemon ne permet pas à chaque domaine WorldClient de posséder son propre certificat : ils doivent donc tous partager le même. Saisissez dans ce champ, en les séparant par des virgules, le nom des autres domaines auxquels les utilisateurs se connecteront et auxquels le certificat s'appliquera. Les caractères jokers sont acceptés. Ainsi, "`*.exemple.com`" s'appliquera à tous les sous-domaines d'`exemple.com` (par exemple, "`wc.exemple.com`", "`mail.exemple.com`", etc).

Taille de la clé de cryptage
Choisissez la longueur, en bits, de la clé de cryptage pour ce certificat. Plus la clé de cryptage est longue, plus le transfert des données est sécurisé. Veuillez noter que toutes les applications ne supportent pas toutes des clés de plus de 512 bits.

Pays
Indiquez dans quel pays se trouve votre serveur.

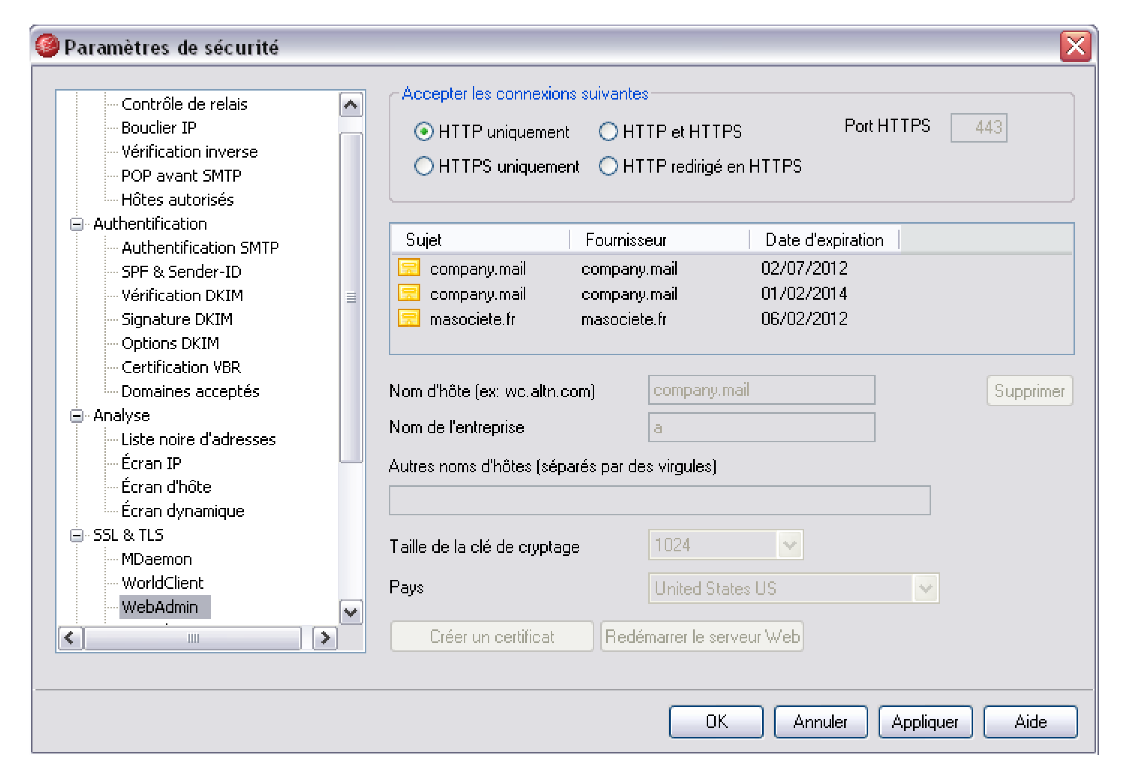
Créer un certificat
Lorsque vous avez saisi toutes les informations requises dans les champs précédents, cliquez sur ce bouton pour créer votre certificat.

Redémarrer le serveur Web
Cliquez sur ce bouton pour redémarrer WorldClient. Il doit être relancé avant l'utilisation des nouveaux certificats.

Voir également :

SSL & Certificats 271
Création et utilisation de certificats SSL 281

4.4.4.3 WebAdmin



Le serveur Web de MDaemon supporte le protocole SSL (Secure Sockets Layer). Le protocole SSL, développé par Netscape Communications Corporation, est la méthode standard pour sécuriser les communications serveur/client sur le Web. Il fournit l'authentification du serveur, le cryptage de données, et l'authentification facultative du client pour la connexion TCP/IP. De plus, dans la mesure où SSL est intégré aux principaux navigateurs actuels, en installant simplement un certificat numérique valide sur votre serveur, les fonctions SSL du client qui se connecte sont activées.

Les options relatives à l'activation et à la configuration de WebAdmin pour qu'il utilise le protocole SSL/HTTPS, se trouvent dans la boîte de dialogue SSL & HTTPS. Pour plus de commodité, ces options sont également accessibles dans la boîte de dialogue Configuration » Services Web, synchro & MI » WebAdmin.

Pour en savoir plus sur ce protocole, voir : **SSL & certificats** 271



Les éléments de cette boîte de dialogue s'appliquent uniquement lorsque WebAdmin utilise le serveur web intégré de MDaemon. Si vous avez configuré WebAdmin pour fonctionner un autre serveur, ces options ne seront alors pas utilisées—le support SSL/HTTPS doit être configuré dans le serveur choisi.

Accepter les connexions suivantes

HTTP uniquement
Sélectionnez cette option si vous ne souhaitez pas autoriser les connexions HTTPS

à WebAdmin. Seules les connexions HTTP seront acceptées.

HTTP et HTTPS
Cette option accepte le support SSL pour WebAdmin, mais les utilisateurs ne sont pas obligés d'employer des connexions HTTPS. Dans ce cas WebAdmin écoute les connexions HTTPS sur le port indiqué dans l'onglet Serveur web 130 des paramètres WebAdmin, mais il répond également aux connexions HTTP normales.

HTTPS uniquement
Avec cette option, il est obligatoire d'utiliser une connexion HTTPS pour se connecter à WebAdmin. Les requêtes HTTP ne sont pas acceptées.

HTTP redirigé en HTTPS
Sélectionnez cette option pour rediriger toutes les connexions HTTP sur le port HTTPS.

Port HTTPS
Il s'agit du port TCP que WebAdmin écoutera pour les connexions SSL. Le port SSL par défaut est le port 443. Si le port SSL par défaut est utilisé, vous n'aurez pas à inclure le numéro du port dans l'URL de WebAdmin lors de la connexion par HTTPS (https://exemple.com est équivalent à https://exemple.com:443).



Le port HTTPS n'est pas le même que celui indiqué dans l'onglet Serveur Web 111 des propriétés de WebAdmin. Si vous autorisez toujours les connexions HTTP vers WebAdmin, ces connexions devront alors utiliser cet autre port pour pouvoir être effectuées correctement. Les connexions HTTPS doivent utiliser le port HTTPS.

Certificats

Cette boîte présente vos certificats SSL. Cliquez une fois sur un certificat pour le sélectionner et l'utiliser. Double-cliquez sur un certificat pour visualiser les détails le concernant dans la boîte de dialogue Certificat.



MDaemon ne permet pas à WorldClient d'utiliser plusieurs certificats. Tous les domaines de WorldClient doivent donc partager un même certificat. Si vous avez plusieurs domaines WorldClient, entrez leur nom (et celui des autres domaines auxquels vous souhaitez autoriser l'accès à WorldClient) dans le champ *Autres noms d'hôtes*, situé en dessous.

Supprimer
Sélectionnez un certificat dans la liste puis cliquez sur ce bouton pour le supprimer. Une boîte de confirmation s'ouvre et vous demande si vous voulez vraiment supprimer ce certificat.

Nom d'hôte
Saisissez le nom de l'hôte auquel vos utilisateurs se connecteront (par exemple, « courrier.exemple.com »).

Nom de l'entreprise
Saisissez le nom de l'organisme ou de la société "propriétaire" du certificat.

Autres noms d'hôtes (séparés par des virgules)
Actuellement, MDaemon ne permet pas à chaque domaine WebAdmin de posséder son propre certificat : ils doivent donc tous partager le même. Saisissez dans ce champ, en les séparant par des virgules, le nom des autres domaines auxquels les utilisateurs se connecteront et auxquels le certificat s'appliquera. Les caractères jokers sont acceptés. Ainsi, "`*.exemple.com`" s'appliquera à tous les sous-domaines d'`exemple.com` (par exemple, "`wc.exemple.com`", " `mail.exemple.com`", etc).

Taille de la clé de cryptage
Choisissez la longueur, en bits, de la clé de cryptage pour ce certificat. Plus la clé de cryptage est longue, plus le transfert des données est sécurisé. Veuillez noter que toutes les applications ne supportent pas toutes des clés de plus de 512 bits.

Pays
Indiquez dans quel pays se trouve votre serveur.

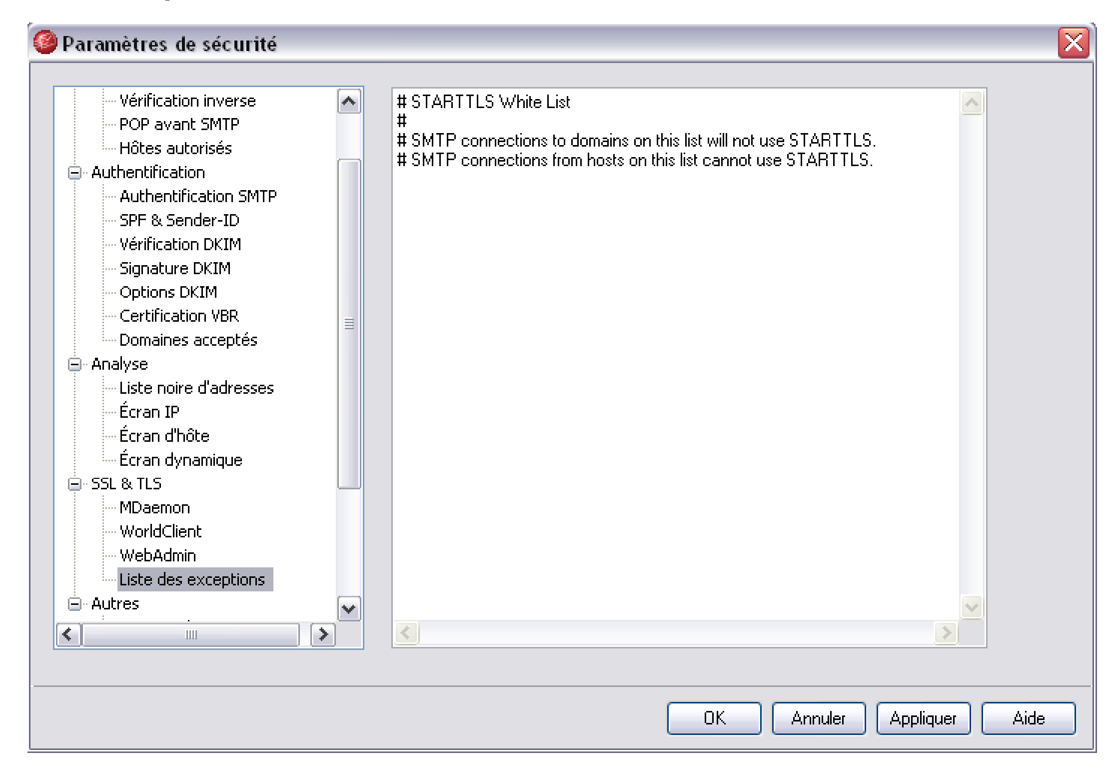
Créer un certificat
Lorsque vous avez saisi toutes les informations requises dans les champs précédents, cliquez sur ce bouton pour créer votre certificat.

Redémarrer le serveur Web
Cliquez sur ce bouton pour redémarrer WorldClient. Il doit être relancé avant l'utilisation des nouveaux certificats.

Voir également :

SSL & Certificats 271
Création et utilisation de certificats SSL 281

4.4.4.4 Liste des exceptions



Cette liste blanche empêche l'utilisation de STARTTLS lors de l'envoi et la réception du courrier depuis certains domaines ou hôtes.

4.4.4.5 Création et utilisation de certificats SSL

Lorsque vous créez des certificats dans la boîte de dialogue SSL & Certificats, MDaemon génère des certificats autosignés. Autrement dit, l'émetteur du certificat ou l'Autorité de Certification (AC) est identique au détenteur du certificat. Cette méthode est autorisée mais, comme l'AC n'est pas répertoriée dans la liste d'AC autorisées, les utilisateurs doivent indiquer s'ils souhaitent ou non accéder au site et/ou installer le certificat pour toute connexion à l'URL HTTPS de WorldClient. Une fois le certificat installé, le domaine de WorldClient est considéré comme une AC valide et le message d'alerte ne s'affiche plus lors de la connexion.

S'ils se connectent à MDaemon via un client de messagerie tel que Microsoft Outlook, il leur est impossible d'installer le certificat. À chaque démarrage du client de messagerie, ils pourront seulement choisir d'utiliser le certificat temporairement, en sachant qu'il n'est pas validé. Pour éviter ce problème, vous devez exporter le certificat et l'envoyer à vos utilisateurs par e-mail pour qu'ils l'installent manuellement, que sa validité soit reconnue et qu'aucun message d'alerte ne soit envoyé.

Créer un certificat

Pour créer un certificat dans MDaemon :

1. Ouvrez la boîte de dialogue SSL & TLS (Sécurité » Paramètres de sécurité » SSL & TLS » MDaemon).

2. Activez l'option *Activer SSL, STARTTLS et STLS*.

3. Dans la zone de texte *Nom d'hôte*, indiquez le domaine auquel appartient le certificat (par exemple, « wc.exemple.com »).

4. Indiquez le nom de la société ou de l'organisation qui détient le certificat dans le champ *Nom de l'entreprise*.

5. Dans *Autres noms d'hôtes*, indiquez le nom des autres domaines dont se serviront vos utilisateurs pour accéder à WorldClient (par exemple, "*.mondomaine.com", "exemple.com", "wc.altn.com", etc.).

6. Choisissez la taille de la clé de cryptage.

7. Choisissez le pays où se trouve votre serveur.

8. Cliquez sur *Créer un certificat*.

Utiliser un certificat créé par une AC tierce

Si vous avez acheté ou généré un certificat depuis une autre source que MDaemon, vous pouvez utiliser ce certificat avec la Console de Gestion Microsoft pour l'importer dans l'emplacement où est stocké le certificat utilisé par MDaemon en procédant comme suit :

1. Dans la Barre d'outils de Windows, cliquez sur **Démarrer > Exécuter**, puis entrez "mmc/a" dans la zone de texte **Ouvrir :**.

2. Cliquez sur **OK**.

3. Dans la Console de Gestion Microsoft, cliquez sur **Fichier > Ajouter/Supprimer un composant logiciel enfichable** (ou appuyez sur Ctrl+M).

4. Dans l'onglet **Autonome**, cliquez sur **Ajouter**.

5. Cliquez sur **Certificats**, puis sur **Ajouter**.

6. Sélectionnez **Compte de l'ordinateur**, puis cliquez sur **Suivant**.

7. Sélectionnez **Ordinateur local**, puis cliquez sur **Terminer**.

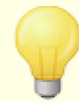
8. Cliquez sur **Fermer**, puis **OK**.

9. Dans **Certificats (Ordinateur Local)**, cliquez sur le dossier **Autorités de certification racine de confiance** , puis sur le sous-dossier **Certificats** si le certificat que vous importez est autosigné. Si ce n'est pas le cas, cliquez sur le dossier **Personnel**.

10. Cliquez sur **Action** > **Toutes les tâches > Importer**, puis sur **Suivant**.

11. Saisissez le chemin d'accès du certificat à importer (cliquez sur **Parcourir** si nécessaire), puis cliquez sur **Suivant**.

12. Cliquez sur **Suivant**, puis sur **Terminer**.



MDaemon n'affiche que les certificats avec des clés privées qui utilisent le format PKCS#12 (Personal Information Exchange). Si le certificat que vous avez importé n'apparaît pas dans la liste, vous devrez importer un fichier *.PEM, qui contient à la fois une clé certifiée et une clé privée. En important ce fichier à l'aide du processus détaillé ci-dessus, il sera converti au format PKCS#12.

Voir également :

SSL & TLS 271

4.4.5 Autres

4.4.5.1 Retours de courrier - Présentation

Retours de courrier

Les "retours de courrier" sont des messages que les utilisateurs reçoivent en réponse à des e-mails qu'ils n'ont jamais envoyés. Cela se produit lorsque des spams ou virus sont envoyés avec une adresse de retour (valeur "Return-path") usurpée. Lorsque l'un de ces messages est rejeté par le serveur du destinataire, ou si le compte a activé un autorépondeur ; la réponse est envoyée à l'adresse usurpée. Le propriétaire de l'adresse reçoit alors des centaines de notifications, messages d'absence, etc., non sollicités. De plus, des spammeurs ou personnes malintentionnées profitent souvent de ce phénomène pour lancer des attaques DoS (Denial of Service) contre les serveurs de messagerie.

Solution

Afin de lutter contre ce problème, MDaemon contient une fonctionnalité appelée "Protection contre les retours de courrier". Cette technologie utilise un système d'algorithmes à clés privées et insère une chaîne spécifique dans la valeur "Return-Path" afin de garantir que les notifications et messages d'autorépondeurs reçus sont légitimes. Ainsi lorsqu'un message envoyé par MDaemon est retourné à l'expéditeur ou déclenche un répondeur automatique, MDaemon identifie le code inséré dans la valeur "Return Path" afin de déterminer si le message d'origine provient de l'un de ses comptes. Si ce code est manquant ou date de plus de 7 jours, l'événement est enregistré dans les journaux de MDaemon et il est possible de rejeter le message.

Ces options sont disponibles en cliquant sur : Sécurité » Paramètres de sécurité » Autres » Retours de courrier.

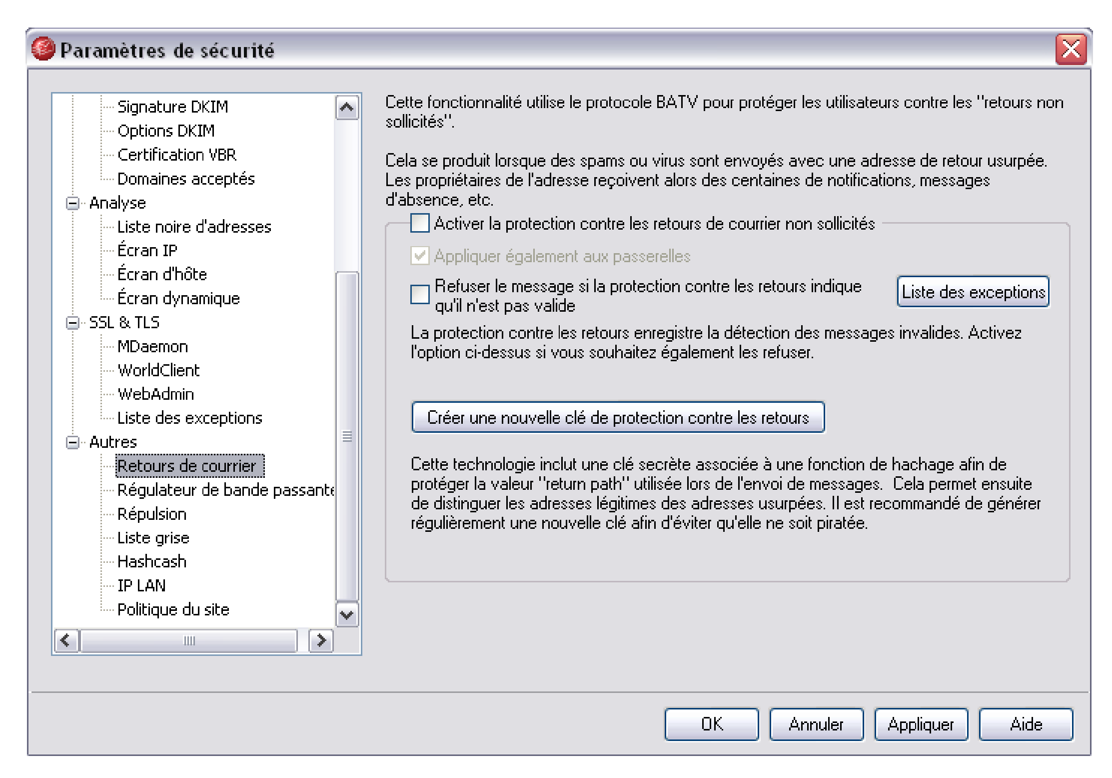
La protection contre les retours de courrier non sollicités s'appuie sur le protocole BATV (Bounce Address Tag Validation). Pour en savoir plus sur ce protocole, consultez (en anglais) :

http://www.mipassoc.org/batv/

Voir également :

Retours de courrier 284

4.4.5.1.1 Retours de courrier



Retours de courrier

Activer la protection contre les retours de courrier non sollicités
Cochez cette option si vous souhaitez insérer un code spécifique dans la valeur "Return-Path" de chaque message sortant. Pour cela, MDaemon utilise la clé privée figurant dans le fichier rsa.private du répertoire PEM/_batv/ de MDaemon. Le code est valide pendant 7 jours. Toutes les notifications de non distribution ou messages d'autorépondeurs doivent contenir un code valide et non expiré. Sinon, la vérification échoue.

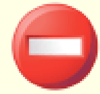


Si cette option n'est pas activée, MDaemon n'insère pas le code spécifique dans les messages sortants. Cependant, il continue à vérifier les notifications de non distribution et messages d'autorépondeurs afin de s'assurer que les messages entrants contenant des codes valides ne sont pas rejetés par

erreur.

Appliquer également aux passerelles
Activez cette option pour appliquer également la protection contre les retours de courrier non sollicités pour les domaines pour lesquels MDaemon est utilisé en tant que passerelle (voir Passerelles de domaine 406).

Refuser le message si la protection contre les retours indique qu'il n'est pas valide
Activez cette option si vous souhaitez refuser les messages pour les lesquels la vérification échoue, c'est à dire si le code inséré dans le message d'origine est manquant ou expiré. Ce système est fiable et n'engendre pas de "faux positifs". Vous pouvez donc activer cette option en toute sécurité. Il suffit que tous les messages envoyés contiennent ce code spécifique. Dans tous les cas, le résultat de la vérification est enregistré dans le journal SMTP-entrant, même si les messages ne sont pas rejetés. Les messages destinés aux passerelles ne sont pas rejetés sauf si l'option *Appliquer également aux passerelles* est activée.



Si vous activez la protection contre les retours de courrier non sollicités, il est recommandé d'attendre au moins une semaine avant de refuser les messages invalides. En effet, vous risquez de recevoir durant cet intervalle des notifications de non distribution ou réponses automatiques à des messages envoyés avant que cette fonctionnalité ne soit activée et des messages légitimes risquent d'être rejetés par erreur. Une fois le délai d'une semaine écoulé, vous pouvez rejeter les messages. Cette recommandation s'applique également lors de la création d'une nouvelle clé (voir ci-dessous).

Liste des exceptions
Cliquez sur ce bouton pour ouvrir la liste blanche de cette fonctionnalité. Elle contient la liste des adresses IP et domaines auxquels la protection contre les retours ne s'applique pas.

Créer une nouvelle clé de protection contre les retours
Cliquez sur ce bouton pour générer une nouvelle clé de protection contre les retours de courrier. Elle est utilisée par MDaemon pour générer les codes spécifiques insérés dans les messages. Cette clé se trouve dans le fichier `rsa.private` du répertoire `PEM/_batv/`de MDaemon. Lors de la création d'une nouvelle clé, un message vous informe que l'ancienne clé continuera de fonctionner pendant 7 jours, sauf si vous choisissez de la supprimer immédiatement. Il est recommandé de ne pas la supprimer immédiatement car des messages légitimes pourraient être refusés.



Si votre trafic est réparti sur plusieurs serveurs, vous devrez probablement partager le fichier contenant la clé avec les autres serveurs ou MTA.

Voir également :

Retours de courrier - Présentation 283

4.4.5.2 Régulation de la bande passante - Présentation

La Régulation de la bande passante permet de maîtriser l'utilisation de la bande passante par MDaemon. Vous pouvez contrôler le taux de progression des sessions et services ; des taux différents peuvent être fixés par domaine (y compris pour le domaine par défaut, les domaines supplémentaires et les passerelles) pour les principaux services de MDaemon. En sélectionnant "Local traffic" dans la liste déroulante, vous pourrez limiter les connexions locales. Ainsi, des paramètres spéciaux de bande passante pourront être créés ; ils s'appliqueront si la connexion provient, ou est en direction d'une adresse IP ou d'un domaine sur le réseau local. Deux zones de textes spéciales ont été créées pour que vous puissiez configurer votre propre liste d'adresses IP et de noms de domaines sur votre réseau local.

La régulation de la bande passante peut s'appliquer par session ou par service. Avec le mode "par session", chaque session est limitée indépendamment à un taux que vous aurez fixé. Ainsi, plusieurs sessions simultanées du même service peuvent dépasser la valeur paramétrée pour la totalité du service. Par contre, si vous configurez la régulation de la bande passante par service, MDaemon contrôle l'utilisation simultanée de toutes les sessions d'un même service, et attribue la même quantité de bande passante à chacune d'entre elles. Les différentes sessions partageront donc, à parts égales, la quantité maximale de bande attribuée. Cela permet de limiter la bande passante pour l'ensemble d'un service.

La régulation de la bande passante est différente selon qu'elle s'applique à une passerelle, qui ne possède pas d'adresse IP spécifique, ou à un domaine. MDaemon doit utiliser la valeur de la commande RCPT pour déterminer si une session SMTP entrante est liée ou non à la passerelle. Si c'est le cas, la régulation de la bande passante SMTP entrante s'applique. De plus, si l'un des destinataires d'un message utilise une passerelle de domaine, la régulation s'applique à toute la session.

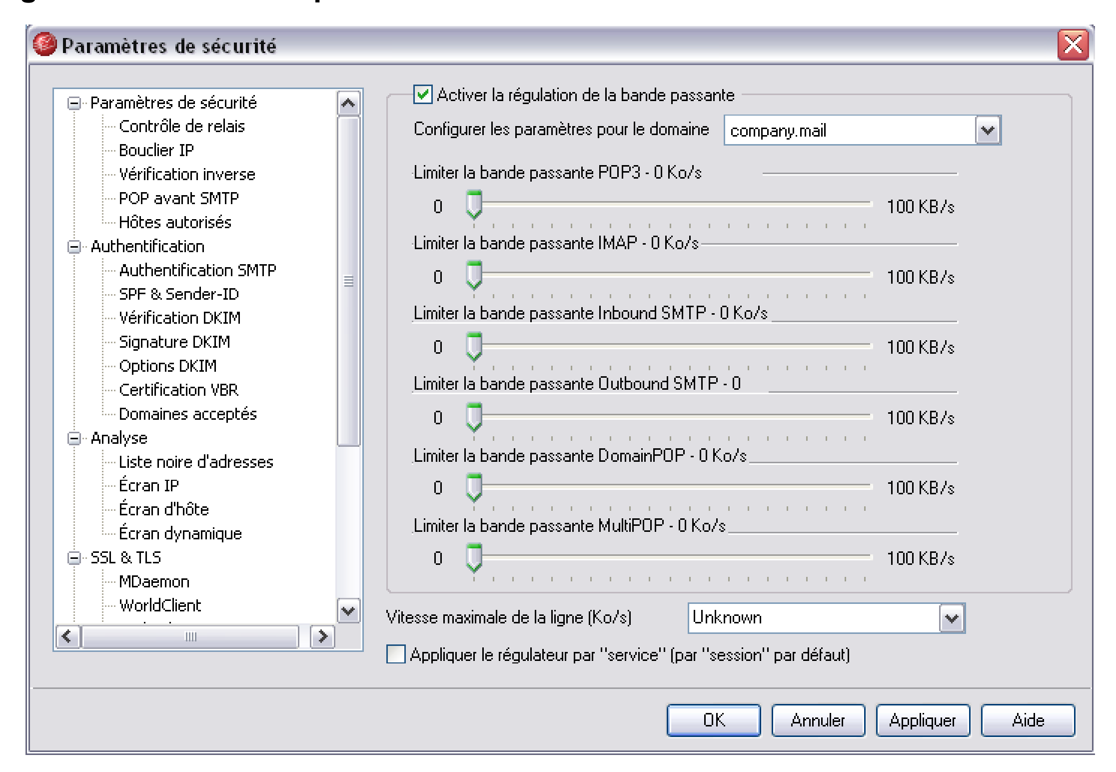
Le système de régulation de la bande passante fonctionne en kilo-octets par seconde (Ko/s). La valeur "0" signifie que la vitesse de progression d'une session (ou d'un service) ne sera pas limitée. La quantité maximale de bande passante disponible pourra être utilisée. Si vous saisissez la valeur "10", par exemple, MDaemon devra volontairement diminuer la vitesse de transmission pour la laisser à 10 Ko/s, ou légèrement au-dessus.

Les pics d'activité au début d'une session entraînent généralement un dépassement des limites fixées. La régulation se met alors en marche et devient plus précise au fur et à mesure de la progression de la session.

Voir également :

Régulation de la bande passante 287
IP LAN 295

4.4.5.2.1 Régulation de la bande passante



Régulateur de bande passante

Activer la régulation de la bande passante
Cochez cette case pour activer le système de régulation de la bande passante.

Configurer les paramètres pour le domaine
Choisissez un domaine dans la liste déroulante, puis modifiez les options correspondant aux différents services pour configurer la régulation de la bande passante pour ce domaine. Si l'une des options est fixée à "0", le service correspondant n'est pas limité en bande passante. Si vous sélectionnez *LocalTraffic*, les limites fixées s'appliqueront au trafic local (c'est-à-dire aux sessions et services uniquement actifs sur votre réseau local). La boîte de dialogue IP LAN 295 répertorie les domaines et adresses IP qui doivent être considérés comme locaux.

Services

Limiter la bande passante [Service] – X KB/s
Lorsque vous avez sélectionné un domaine dans la liste déroulante, modifiez ces commandes pour définir les limitations de bande passante pour ce domaine. Si vous fixez la valeur "0" pour un service, celui-ci ne sera pas limité en bande passante. Si le curseur est placé sur un autre nombre, la bande passante pour le service concerné, sera limitée à cette valeur en kilo-octets par seconde.

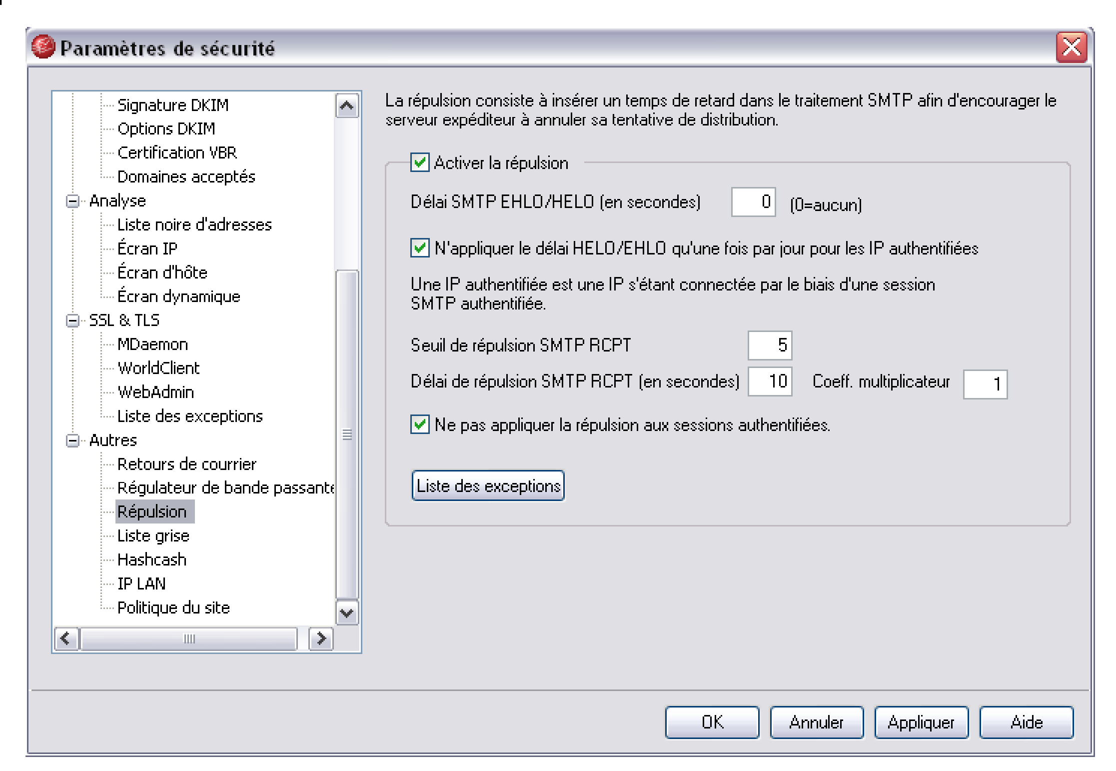
Vitesse maximale de la ligne (Ko/s)
Sélectionnez dans la liste déroulante, la vitesse maximale de votre connexion, en kilo-octets par seconde.

Appliquer le régulateur par "service" (par "session" par défaut)
Activez cette option pour que le régulateur s'applique "par service" et non "par session". Lorsque la régulation s'effectue par service, la quantité de bande passante attribuée à un service sera partagée de façon égale entre toutes des sessions actives du service en question. Ainsi, la quantité totale de bande utilisée par plusieurs clients IMAP qui se connectent simultanément, par exemple, ne pourra jamais dépasser la quantité définie, quel que soit le nombre de clients connectés. Si la régulation s'applique par session, aucune session IMAP ne pourra dépasser la limite fixée, mais plusieurs sessions simultanées le pourront.

Voir également :

Régulation de la bande passante - Présentation 286

4.4.5.3 Répulsion



Cette boîte de dialogue se trouve dans : Sécurité » Paramètres de sécurité » Autres » Répulsion.

La répulsion permet de ralentir délibérément une connexion lorsque le nombre de commandes RCPT que vous avez indiquées ont été reçues de l'expéditeur d'un message. Cela permet de dissuader les spammeurs de tenter d'utiliser votre serveur pour envoyer en masse du spam. Vous pouvez spécifier le nombre de commandes RCPT autorisées avant que la répulsion commence et le nombre de secondes de délai, chaque fois qu'un hôte envoie une commande au cours de la même connexion. Cette technique suppose que si l'envoi de chaque message nécessite une durée anormalement longue, les spammeurs seront dissuadés de tenter d'utiliser votre serveur

à l’avenir.

Activer la répulsion
Cochez cette case pour activer les fonctions de répulsion de MDaemon.

Délai SMTP EHLO/HELO (en secondes)
Cochez cette option pour retarder la réponse aux commandes SMTP EHLO/HELO. Il suffit de retarder cette réponse de dix secondes pour réduire considérablement le nombre de spams reçus. En effet, les spammeurs doivent souvent envoyer les messages rapidement et n’attendent pas longtemps la réponse aux commandes EHLO/HELO. Ce délai ne s’applique pas aux connexions sur le port MSA (défini dans l’onglet Ports 41 du Domaine par défaut 32).Paramètre par défaut : 0 (aucun délai).

N’appliquer le délai EHLO/HELO qu’une fois par jour pour les IP authentifiées
Lorsque cette option est activée, le délai EHLO/HELO ne s’applique pas plus d’une fois par jour pour les sessions connectées avec une adresse IP authentifiée.

Seuil de répulsion SMTP RCPT
Indiquez le nombre de commandes SMTP RCPT que vous souhaitez autoriser pour un hôte donné, lors d’une session de messagerie, avant que MDaemon ne commence la répulsion de cet hôte. Par exemple, si ce nombre est défini sur 10 et qu’un hôte tente d’envoyer un message à 20 adresses (c’est-à-dire 20 commandes RCPT), MDaemon autorisera alors les 10 premières normalement et introduira, entre chaque commande qui suit, un temps de pause, égal au nombre de secondes que vous avez indiqué dans le champ *Délai de répulsion SMTP RCPT* ci-dessous.

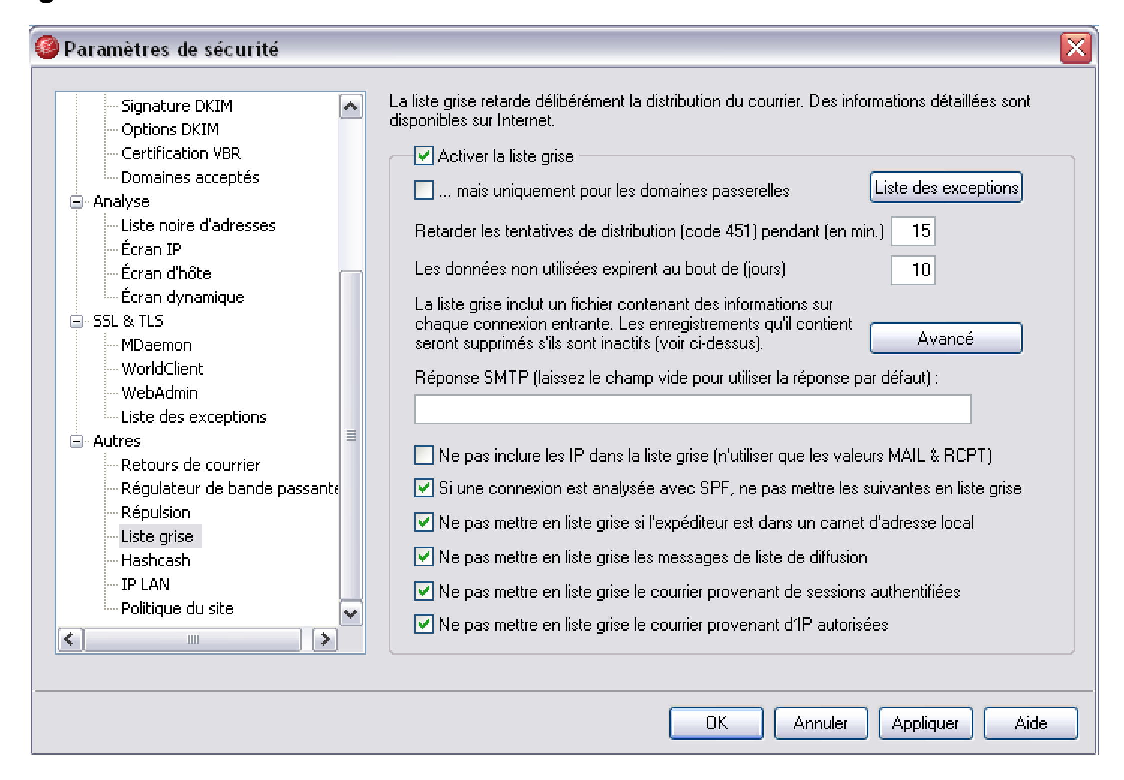
Délai de répulsion SMTP RCTP (en secondes)
Une fois que le Seuil de répulsion SMTP RCTP est dépassé pour cet hôte, la valeur saisie dans ce champ correspond au temps de pause (en secondes) que MDaemon introduit entre chaque commande RCPT qu’il reçoit de cet hôte lors de la session de messagerie.

Coeff. multiplicateur
Ce coefficient augmente la durée du délai. Lorsque le seuil est atteint et que le délai de répulsion s'applique à une session, sa durée est multipliée par cette valeur afin de déterminer le délai de la session suivante. Par exemple, si le délai SMTP RCPT est de 10 secondes et que le coefficient multiplicateur est 1.5 ; le premier délai est de 10 secondes, le deuxième de 15 secondes (10x1,5), le troisième de 22,5 (15x15,5), etc. Valeur par défaut : 1 (la durée du délai n'est jamais augmentée).

Ne pas appliquer la répulsion aux sessions authentifiées
Activez cette option pour que les expéditeurs utilisant des sessions de messagerie authentifiées ne soient pas soumis aux paramètres de répulsion.

Liste des exceptions
Cliquez sur ce bouton pour définir la liste des adresses IP auxquelles la répulsion ne s'applique pas.

4.4.5.4 Liste grise



La liste grise est une technique de lutte contre le spam consistant à renvoyer une erreur temporaire aux serveurs SMTP envoyant du courrier à MDaemon afin qu'ils renouvellement la tentative ultérieurement. Ainsi, les messages reçus d'un expéditeur inconnu ou ne figurant pas sur la liste blanche sont temporairement refusés au cours de la session SMTP, et le destinataire et l'adresse IP de l'expéditeur sont enregistrés. De plus, toute tentative de distribution de cet expéditeur sera également refusée pendant une période définie. Cette méthode a pour but de réduire le nombre de spams reçus par les utilisateurs, car les spammeurs ne renouvellent généralement pas les tentatives d'envoi lorsqu'un message est refusé. Cependant, cette technique peut également retarder la distribution du courrier légitime. Même si les messages légitimes sont distribués une fois le délai de la liste grise expiré, il est impossible de déterminer à quel moment ils seront renvoyés. Un message refusé temporairement par la liste grise peut aussi bien être retardé de quelques minutes que d'une journée entière.

Cet onglet contient diverses options destinées à éviter les inconvénients de la liste grise.

Par exemple, un problème se présente lorsque le domaine expéditeur possède un pool de serveurs pour l'envoi du courrier, car un serveur différent est utilisé pour chaque envoi. Par conséquent, le moteur de la liste grise considère chaque envoi comme une nouvelle connexion, ce qui augmente considérablement le temps d'attente. Afin de résoudre ce problème, une option SPF a été ajoutée à la liste grise. Ainsi, si le domaine expéditeur publie des enregistrements SPF lors du premier envoi, les envois suivants ne seront pas mis en liste grise. De plus, une autre option permet d'ignorer l'adresse IP du serveur expéditeur. Cela réduit l'efficacité de la liste grise mais résout entièrement le problème mentionné ci-dessus.

D'autre part, les listes grises comprennent généralement des bases de données

volumineuses car chaque connexion entrante est analysée. C'est pourquoi, dans MDaemon cette fonctionnalité s'effectue quasiment à la fin du processus de traitement du courrier. Les messages sont ainsi soumis à l'analyse des autres outils et éventuellement rejetés avant d'atteindre la liste grise, ce qui réduit la taille de sa base de données. Le programme étant résident, cela n'a que peu de conséquences sur les performances de l'ordinateur.

Des options avancées de liste blanche réduisent le nombre de messages légitimes mis en liste grise. Il existe pour cela un fichier spécifique mais il est également possible de considérer comme "liste blanche" le fichier contenant votre carnet d'adresses privé. Dans ce cas, les messages provenant d'utilisateurs figurant dans ce carnet ne sont pas soumis à la liste grise. Vous pouvez également exclure de la liste grise les messages des listes de diffusion. Enfin, le fichier de base de données se met automatiquement à jour en supprimant les entrées qui n'ont pas été utilisées pendant une certaine période.

Plus d'informations sur les listes grises sont disponibles (en anglais) à l'adresse :

http://projects.puremagic.com/greylisting/

Paramètre de la liste grise

Activer la liste grise
Cochez cette case pour activer les fonctionnalités de la liste grise.

...mais uniquement pour les domaines passerelles
Cochez cette case si vous ne souhaitez appliquer la liste grise qu'aux messages destinés aux passerelles.

Liste des exceptions
Indiquez dans ce fichier les destinataires et adresses IP pour lesquels la liste grise ne s'applique pas.

Retarder les tentatives de distribution (code 451) pendant (en min.)
Nombre de minutes pendant lequel un message est retardé. Une fois le message temporairement rejeté, toute tentative d'envoi contenant les mêmes paramètres serveur/expéditeur/destinataire sera refusée pendant la période indiquée. Après cette période, aucun délai ne sera appliqué à cet expéditeur jusqu'à l'expiration de la base de données de la liste grise.

Les données non utilisées expirent au bout de (jours)
Lorsque la période de délai est expirée, les messages provenant du même serveur et envoyés au même destinataire ne sont plus rejetés. Cependant, si aucun message n'est reçu pendant le nombre de jours indiqués l'enregistrement de la base de données expire et la liste grise s'applique à nouveau.

Avancé
Cliquez sur ce bouton pour ouvrir la base de données de la liste grise.

Réponse SMTP (laissez le champ vide pour utiliser la réponse par défaut) :
Si vous saisissez du texte ici, MDaemon renvoie la réponse SMTP, "`451 <votre`

`message>`" au lieu de "`451 Liste grise activée, veuillez réessayer dans X minutes`." Cela peut être utile si vous souhaitez par exemple inclure une URL pointant vers une description du système de liste grise.

Ne pas inclure les IP dans la liste grise (n'utiliser que les valeurs MAIL & RCPT)
Cochez cette option si vous souhaitez que la liste grise ne prenne pas en compte l'adresse IP du serveur. Cela permet de résoudre les problèmes éventuels liés aux pools de serveurs mais réduit l'efficacité du système.

Si une connexion est analysée avec SPF, ne pas mettre les suivantes en liste grise
Avec cette option, lorsque l'enregistrement d'un serveur expéditeur a déjà été vérifié par SPF, les connexions suivantes ne sont pas mises en liste grise.

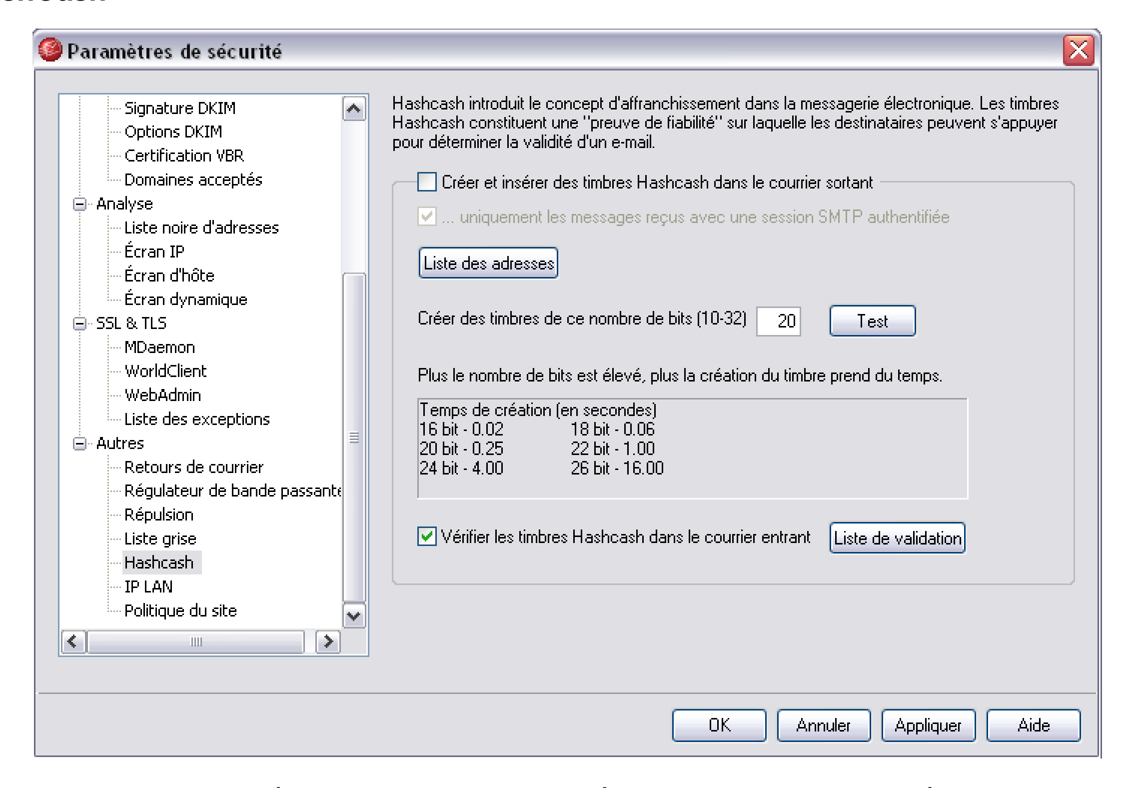
Ne pas mettre en liste grise si l'expéditeur est dans un carnet d'adresses local
Cochez cette case si vous ne souhaitez pas appliquer la liste grise aux messages dont l'expéditeur figure dans le carnet d'adresses du destinataire.

Ne pas mettre en liste grise les messages de liste de diffusion
Cochez cette case si vous ne souhaitez pas appliquer la liste grise aux messages de liste de diffusion.

Ne pas mettre en liste grise le courrier provenant de sessions authentifiées
Cochez cette case si vous ne souhaitez pas appliquer la liste grise aux messages provenant de sessions authentifiées.

Ne pas mettre en liste grise le courrier provenant d'IP autorisées
Cochez cette option si vous ne souhaitez pas appliquer la liste grise aux messages provenant d'IP autorisées.

4.4.5.5 HashCash



HashCash est un système d'affranchissement électronique permettant à la fois de lutter contre le spam et les attaques par déni de service. Il génère des timbres virtuels ("payés" avec du temps processeur), qui sont insérés dans les en-têtes des messages sortants puis vérifiés par le serveur du destinataire. Les messages comportant un timbre ont donc de fortes chances d'être légitimes, c'est pourquoi ils sont acceptés par les systèmes anti-spam. Le système HashCash réduit le nombre de faux positifs et évite que certains messages soient rejetés par erreur par des filtres ou des listes noires.

Les spammeurs profitent de techniques telles que le CCI (Copie carbone invisible, BCC en anglais) pour envoyer des centaines, voire des milliers d'exemplaires du même message en un temps très court. Or, un spammeur souhaitant utiliser le système HashCash devrait créer un timbre unique pour chaque message et chaque destinataire, ce qui s'avère très décourageant ! En revanche, pour un utilisateur moyen, le temps processeur nécessaire pour attribuer un timbre aux messages sortants est généralement insignifiant. De plus, les messages issus des listes de diffusion ne sont pas concernés par ce système.

Les timbres ne sont crées que pour les messages sortants distants provenant des/ destinés aux adresses de la "Liste des adresses", et les listes de diffusion sont toujours exclues. Par défaut, MDaemon ne crée de timbres que pour les messages provenant d'une session SMTP authentifiée. Vous pouvez désactiver cette option mais cela n'est pas recommandé.

Pour les messages entrants, seuls les timbres des messages dont le destinataire figure dans la "Liste de validation" sont vérifiés. Si un message entrant contient un timbre HashCash mais que son destinataire n'est pas sur la liste, le timbre est ignoré et le message distribué normalement. Par défaut, seul le domaine primaire figure sur cette

liste. Cliquez sur le bouton "Liste de validation" pour y ajouter des domaines supplémentaires ou des passerelles.

Pour plus d'informations sur le système HashCash, consultez : http://www.hashcash.org/.

HashCash

Créer et insérer des timbres HashCash dans le courrier sortant
Active le système HashCash, des timbres sont attribués aux messages sortants distants provenant des/destinés aux adresses de la "Liste des adresses".

...uniquement pour les messages reçus avec une session SMTP authentifiée
Seuls les messages provenant de sessions SMTP authentifiées sont marqués. Il est recommandé de ne pas décocher cette option.

Liste des adresses
Ouvre la liste des adresses pour lesquelles des timbres sont créés. Par défaut, seul le domaine principal y figure, mais vous pouvez y ajouter des domaines supplémentaires, passerelles, ou des adresses spécifiques.

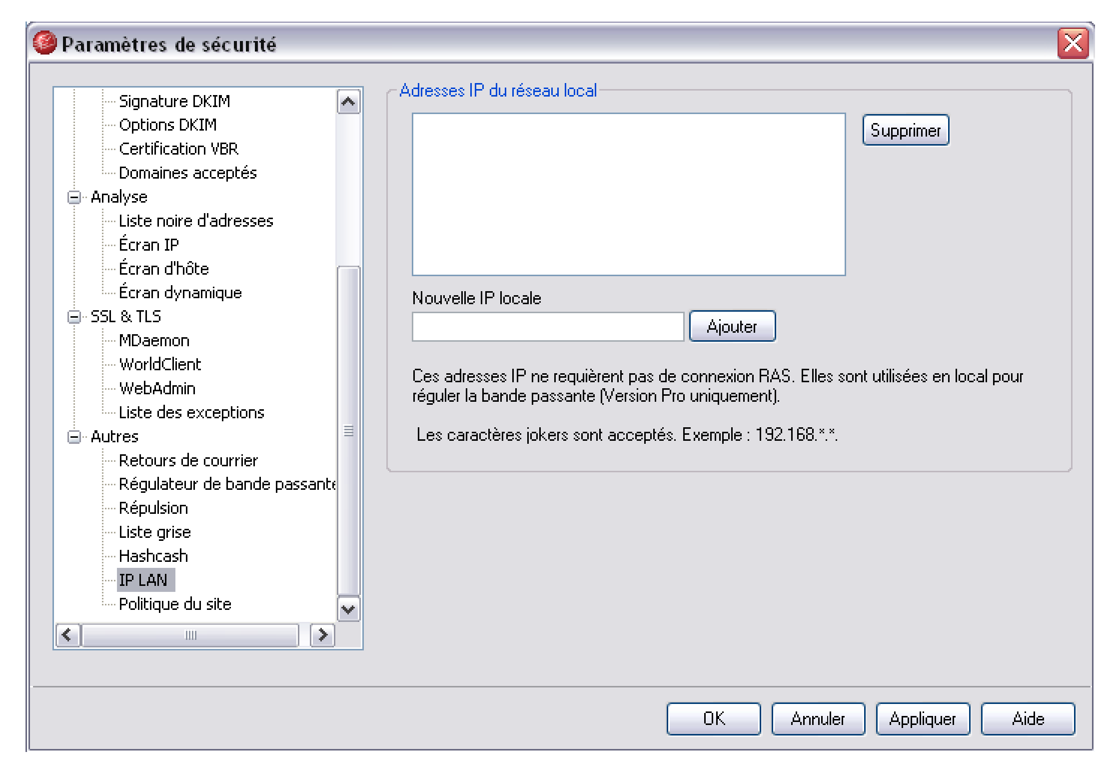
Créer des timbres de ce nombre de bits (10-32)
Nombre de bits utilisés pour créer un timbre. Plus ce nombre est élevé, plus le temps processeur nécessaire est important.

Test
Teste le temps nécessaire à la création d'un timbre en fonction du nombre de bits.

Vérifier les timbres HashCash dans le courrier entrant
Vérifie les timbres des messages entrants et ajuste leur score spam selon le résultat. Seuls les timbres des messages dont le destinataire figure dans la "Liste de validation" seront vérifiés. Si un message entrant contient un timbre HashCash mais que son destinataire n'est pas sur la liste, le timbre sera ignoré et le message distribué normalement.

Liste de validation
Liste des destinataires pour lesquels les timbres HashCash sont vérifiés. Les messages entrants dont les destinataires ne figurent pas sur la liste seront distribués normalement. Par défaut, seul le domaine primaire y figure.

4.4.5.6 IP LAN



Remarque : Cette boîte de dialogue est identique à celle du même nom, situées dans les Paramètres de connexion RAS 88. Toute modification effectuée dans l'une de ces boîtes de dialogue apparaîtra également dans l'autre.

Adresses IP du réseau local

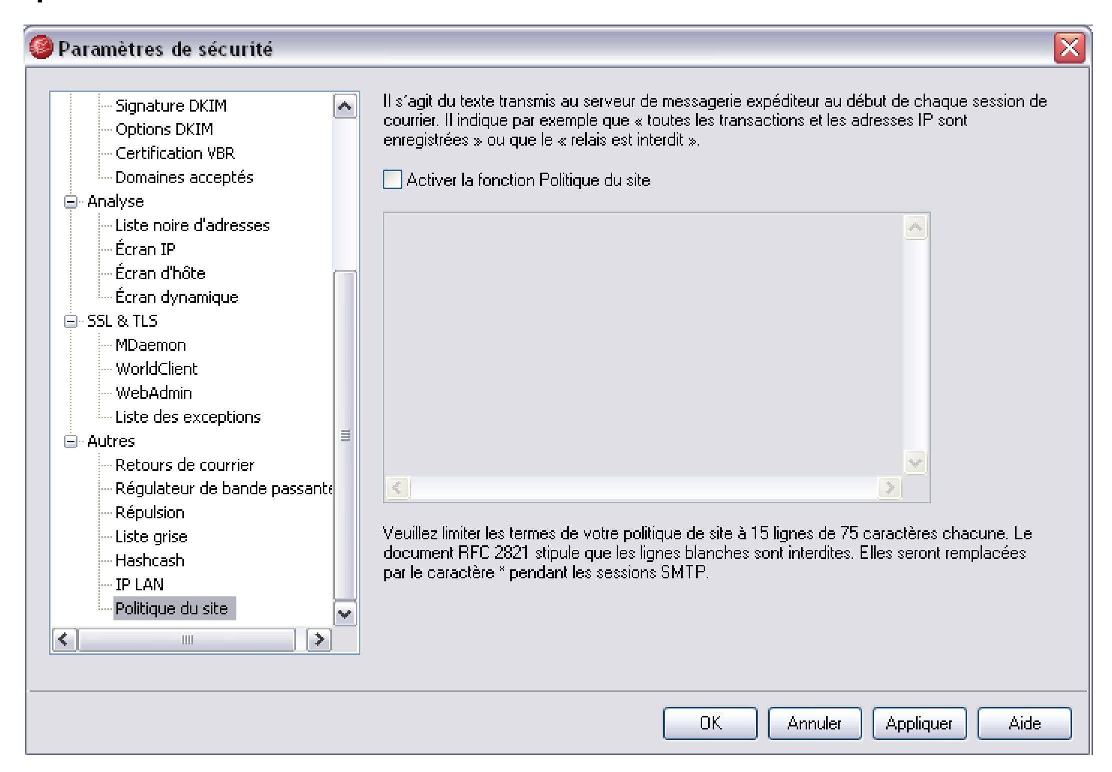
Cet onglet sert à répertorier les adresses IP situées sur votre réseau local. Ces IP ne requièrent donc pas de connexion RAS et sont considérées comme locales par le système de régulation de la bande passante. De plus, plusieurs autres restrictions concernant la sécurité et les mesures de prévention du spam ne sont pas appliquées à ces adresses.

Supprimer
Pour supprimer une adresse IP de la liste, sélectionnez-la et cliquez sur ce bouton.

Nouvelle IP locale
Saisissez une adresse IP à ajouter à la liste des IP locales puis cliquez sur Ajouter. Les caractères jokers tels que 127.0.*.* sont acceptés.

Ajouter
Lorsque vous avez saisi une adresse IP dans le champ ci-dessus, cliquez sur ce bouton pour l'ajouter à la liste.

4.4.5.7 Politique du site



Activer la fonction Politique du site
Le texte de votre politique de site est enregistré dans le fichier policy.dat (sous-répertoire \App\ de MDaemon). Il est transmis aux serveurs d'envoi au début de chaque session SMTP. Cette politique de site peut être, par exemple, "Ce serveur n'est pas un relais" ou "Utilisation interdite sans autorisation". Il est inutile de précéder les lignes par "220" ou "220-", MDaemon les traite en avec ou sans ces codes.

Exemple de politique de site lors d'une transaction SMTP :

```
220-Alt-N Technologies ESMTP MDaemon
220-Ce site ne relaye pas le courrier non autorisé.
220-Si vous n'êtes pas un utilisateur autorisé sur notre serveur
220-vous ne devez pas utiliser ce site pour envoyer du courrier.
220
HELO domain.com...
```

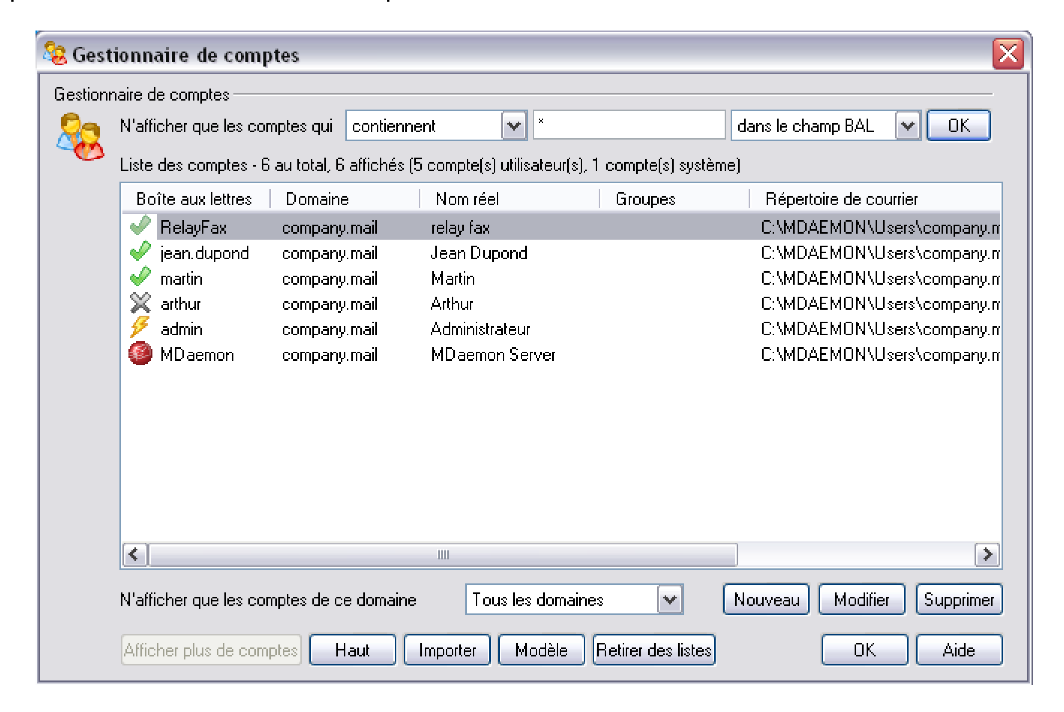
Le fichier POLICY.DAT se compose en texte Ascii et contient 512 caractères maximum par ligne ; nous vous conseillons toutefois de ne pas dépasser 75 caractères par ligne. La taille maximale du fichier s'élève à 5000 octets. MDaemon n'affichera pas les fichiers qui dépassent cette taille.

Section V

5 Menu Comptes

5.1 Gestionnaire de comptes

Afin de mieux gérer la sélection, l'ajout, la suppression ou la modification de vos comptes, MDaemon contient un Gestionnaire de comptes. Cette boîte de dialogue permet d'accéder aux informations de compte et sert à trier les comptes par boîte, domaine, par nom réel ou par répertoire de courrier. Pour y accéder, cliquez sur : Comptes » Gestionnaire de comptes...



Gestionnaire de comptes

Au dessus de la liste de comptes, vous trouverez les deux statistiques concernant la liste. Le premier chiffre correspond au nombre total de comptes utilisateur MDaemon qui existent actuellement sur votre système. Le second chiffre correspond au nombre de comptes actuellement affichés dans la liste de comptes. Le nombre de comptes affichés dépend de la valeur sélectionnée dans le menu déroulant *N'afficher que les comptes de ces domaines.* Si vous avez sélectionné *"Tous les Domaines",* tous vos comptes MDaemon s'affichent. Le champ de recherche situé au -dessus de la liste permet de filtrer les comptes affichés en fonction de critères spécifiques.

Chaque entrée de la liste de comptes comporte : une icône d'état, le domaine auquel appartient le compte, la boîte aux lettres, le nom réel de l'utilisateur, les éventuels groupes auxquels il appartient ainsi que le répertoire de courrier. Cette liste peut être classée par ordre croissant ou décroissant en fonction de vos préférences. Cliquez sur l'une des colonnes pour classer la liste par ordre croissant dans la colonne. Cliquez à nouveau sur la colonne pour la trier par ordre décroissant.



Par défaut, seuls 500 comptes peuvent être affichés dans cette liste. Si vous souhaitez afficher plus de comptes à partir du domaine actuellement sélectionné (ou tous les domaines, si vous avez sélectionné cette option), vous devez alors cliquer sur le bouton *Afficher plus de comptes* pour afficher les 500 prochains comptes. Si vous voulez pouvoir afficher plus de 500 comptes simulatnément, ouvrez le fichier MDaemon.ini et saisissez la valeur que vous souhaitez dans la clé `MaxAccountManagerEntries=500`.

Icônes d'état des comptes

Administrateur global ou de domaine.

Accès complet : POP et IMAP.

Accès limité. L'un des services POP ou IMAP est désactivé.

Accès limité. Les services POP et IMAP sont tous deux désactivés.

Compte désactivé. L'utilisateur ne peut pas y accéder.

Compte système de MDaemon.

N'afficher que les comptes de ce domaine
Sélectionnez *Tous les domaines* dans la liste pour afficher tous les comptes MDaemon. Choisissez un domaine spécifique pour n'afficher que les comptes de ce domaine.

Nouveau
Cliquez sur ce bouton pour ouvrir l'Éditeur de comptes 301 et créer un nouveau compte.

Modifier
Sélectionnez un compte à partir de la liste de comptes, puis cliquez sur ce bouton pour l'ouvrir dans l'Éditeur de comptes 301.

Supprimer
Pour supprimer un compte, sélectionnez-le et cliquez sur ce bouton (un écran de confirmation s'affiche).

Afficher plus de comptes
La liste de comptes n'affiche que 500 comptes simultanément. S'il y a plus de 500 comptes dans le domaine que vous avez sélectionné, cliquez sur ce bouton pour afficher les 500 prochains comptes. Reportez-vous à la remarque ci-dessus pour obtenir des instructions sur la façon d'augmenter le nombre de comptes qui

s’afficheront.

Haut
Cliquez sur ce bouton pour atteindre le début de la liste de comptes.

Importer
Cliquez sur ce bouton pour importer des comptes depuis un fichier séparé par des virgules. Cette option est également disponible en cliquant sur Comptes » Importer » Importer les comptes à partir d'un fichier texte délimité par des virgules.

Modèle
Cliquez sur ce bouton pour ouvrir la boîte de dialogue Modèle de compte330.

Retirer des listes
Si vous souhaitez désinscrire des comptes de toutes les listes de diffusion381 du serveur, sélectionnez-les et cliquez sur ce bouton. Une fenêtre de confirmation s'affiche alors

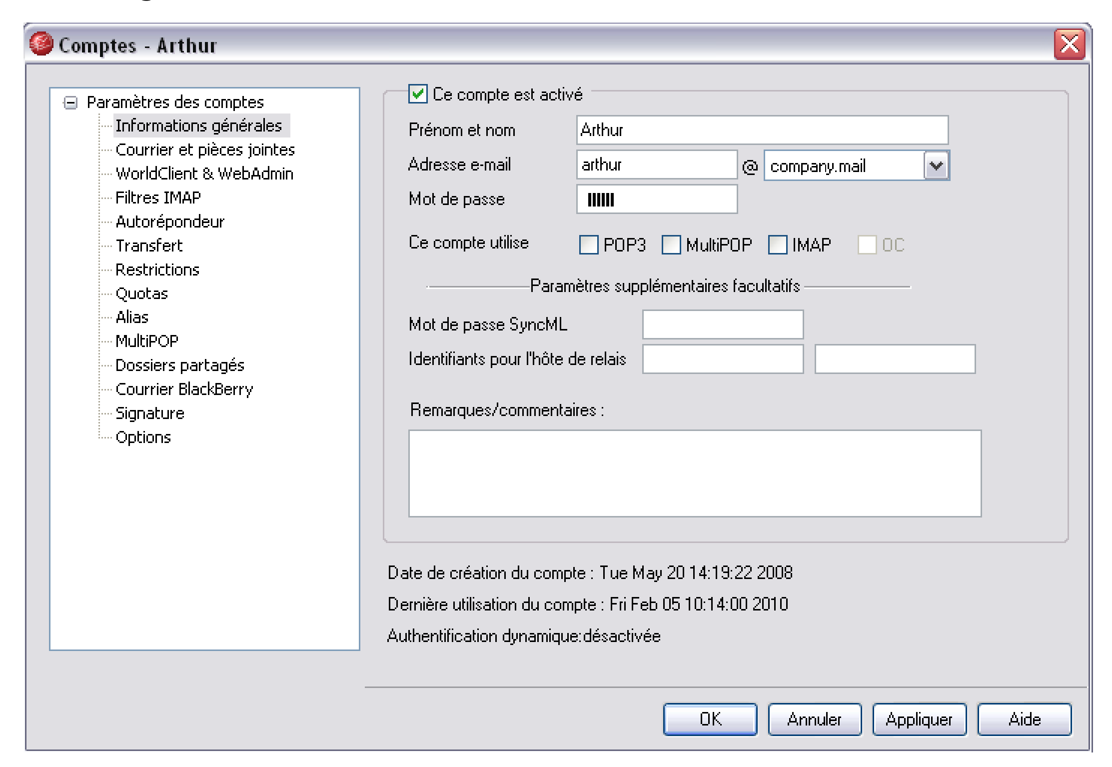
---

Voir également :

Modèles pour les nouveaux comptes330
Éditeur de comptes301

5.1.1 Éditeur de comptes

5.1.1.1 Informations générales



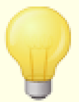
Compte

Ce compte est activé
Cochez cette case pour activer tous les accès de ce compte. Si vous la décochez, l'utilisateur ne pourra plus accéder à son compte, de quelque façon de ce soit, et MDaemon n'acceptera plus le courrier qui lui est destiné. Le serveur agira comme si le compte n'existait plus. Cependant, il sera toujours inclus dans le calcul du nombre de comptes autorisé par le licence.

Prénom et nom
Entrez ici le nom et prénom de l'utilisateur. Lors de la création d'un nouveau compte, la plupart des champs sont remplis automatiquement en fonction des paramètres du Modèle de compte 330. Ce champ ne doit pas contenir les caractères " ! " ou " | ".

Adresse e-mail
Adresse e-mail du compte. Ce champ se remplit automatiquement avec la valeur saisie dans le champ *Prénom et nom*, en fonction des paramètres du Modèle de compte 330, mais vous pouvez saisir la valeur de votre choix. Sélectionnez ensuite un domaine dans le menu déroulant situé après le caractère @ (par défaut, le domaine sélectionné est le Domaine par défaut 33 de MDaermon). L'adresse e-mail complète sert d'identifiant unique POP3, IMAP, WorldClient, etc. Les adresses e-mail ne doivent pas contenir d'espaces ou de caractères "!" ou"|".

Mot de passe
Mot de passe du compte. L'Éditeur indique si ce mot de passe utilise l' authentification dynamique 372.



Vous devez toujours fournir un mot de passe, même si vous ne souhaitez pas autoriser l'accès POP/IMAP au compte de messagerie. En plus de la vérification de session POP, l'adresse e-mail et le mot de passe permettent d'autoriser les manipulations de compte et le retrait de fichiers à distance. Si vous souhaitez interdire l'accès POP/IMAP ou Outlook Connector, décochez les options correspondantes.

Ce compte utilise :

POP3
Décochez cette case si vous ne souhaitez pas que l'utilisateur puisse accéder à son compte avec le protocole POP. Il pourra toujours y accéder par IMAP, WorldClient, ou WebAdmin si les options correspondantes sont activées.

MultiPOP
Cochez cette case si vous souhaitez autoriser le compte à utiliser MultiPOP 320.

IMAP
Décochez cette case si vous ne souhaitez pas que l'utilisateur puisse accéder à son compte avec le protocole IMAP. Il pourra toujours y accéder par POP, WorldClient, ou WebAdmin si les options correspondantes sont activées.

Outlook Connector
Sélectionnez cette option pour autoriser le compte à partager les dossiers Microsoft Outlook avec les utilisateurs de Outlook Connector for MDaemon 356.
Remarque : cette option est disponible uniquement lorsque Outlook Connector est installé.

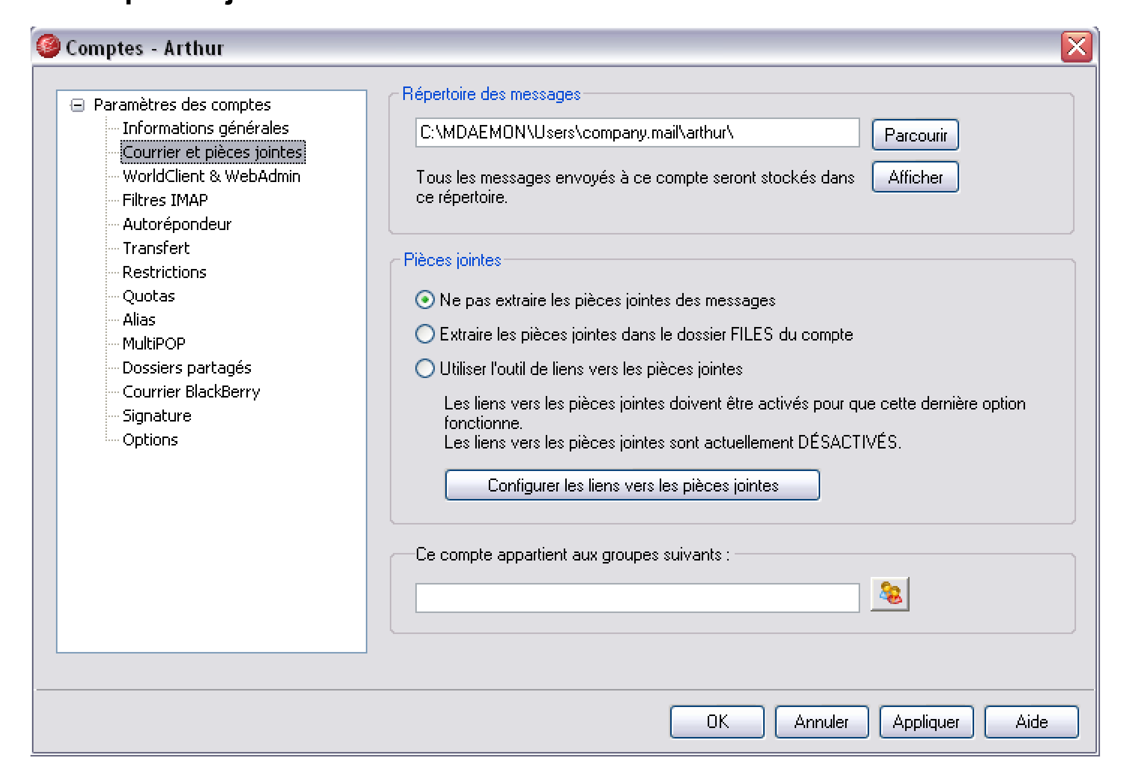
Mot de passe SyncML
Utilisez cette option si vous souhaitez indiquer un mot de passe différent lors des connexions au serveur SyncML 122. Si ce champ n'est pas rempli, le mot de passe du compte est utilisé. Cependant, les comptes utilisant l'authentification dynamique doivent posséder un mot de passe spécifique pour le serveur SyncML.

Mot de passe de l'hôte de relais
Si l'option *Autoriser une authentification par compte* est activée dans l'onglet Distribution 34 des paramètres du domaine par défaut, indiquez ici le mot de passe du compte pour l'authentification sur l'hôte de relais. Ne remplissez pas ce champ si vous ne souhaitez pas utiliser une authentification spécifique pour ce compte.

Remarques/commentaires

Utilisez cette zone de texte pour ajouter des notes ou des commentaires concernant ce compte.

5.1.1.2 Courrier et pièces jointes



Répertoire des messages

Indiquez le répertoire dans lequel seront placés les messages entrants destinés à la boîte aux lettres de ce compte (l'emplacement par défaut est défini dans le Modèle de compte 330.

Pièces jointes

Ne pas extraire les pièces jointes des messages
Si cette option est sélectionnée, les pièces jointes ne sont pas extraites et les messages sont distribués normalement.

Extraire les pièces jointes dans le dossier FILES du compte
Si ce paramètre est activé, MDaemon extrait automatiquement les pièces jointes des messages entrants. Les fichiers extraits sont retirés des messages entrants et placés dans le répertoire \Files\ du compte (par défaut : C:\MDaemon\Users\<domaine>\<utilisateur>). Le corps du message indique les noms des fichiers extraits mais aucun lien n'est fourni pour les récupérer. L'utilisateur doit donc disposer d'un accès au dossier \Files\ de son compte.

Utiliser l'outil de liens vers les pièces jointes
Cette option extrait les pièces jointes des messages et les stocke à l'emplacement désigné dans la fenêtre Liens vers les pièces jointes 139. Le corps du message contient des liens permettant à l'utilisateur de récupérer les pièces jointes extraites. Pour des raisons de sécurité, ces URL ne contiennent pas de chemins complet, mais un identifiant unique (GUID) que le serveur utilise pour lier le fichier. Les liaisons

GUID sont définies dans le fichier `AttachmentLinking.dat`.



Si cette option est sélectionné, mais que le système n'est pas activé dans la fenêtre Liens vers les pièces jointes 139, les pièces jointes ne seront pas extraites.

Configurer les liens vers les pièces jointes
Cliquez sur ce bouton pour ouvrir la fenêtre Liens vers les pièces jointes 139.

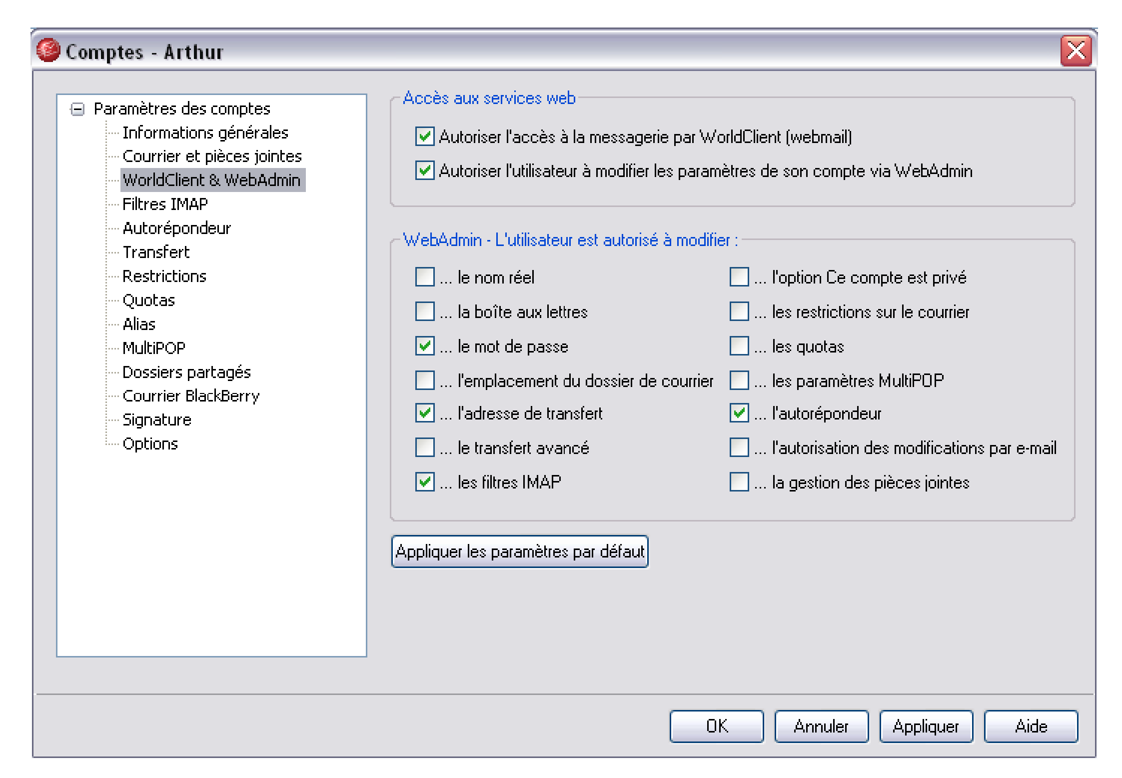
Groupes

Ce compte appartient aux groupes suivants :
Ce champ permet d'inclure le compte dans un ou plusieurs Groupes 368. Vous pouvez également cliquer sur l'icône pour consulter la liste des groupes disponibles.

Voir également :

Liens vers les pièces jointes 303
Modèle de compte 330
Groupes 368

5.1.1.3 WorldClient & WebAdmin



Accès aux services web

Autoriser l'accès à la messagerie par WorldClient
Activez cette option si vous voulez que l'utilisateur puisse accéder au serveur WorldClient 106, et ainsi consulter son courrier dans un navigateur web.

Autoriser l'utilisateur à modifier les paramètres de son compte via WebAdmin
Activez cette option si vous souhaitez autoriser l'utilisateur à modifier les paramètres de son compte via WebAdmin 129. Cochez ensuite les cases correspondant aux paramètres que l'utilisateur peut modifier.

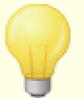
Lorsque cette fonctionnalité est activée et que le serveur WebAdmin est activé, l'utilisateur peut se connecter à WebAdmin à l'aide de son navigateur sur le port attribué à WebAdmin 130 (ex. : `http://exemple.com:1000`). Après un premier écran d'identification, un second écran s'affiche contenant les paramètres que l'utilisateur peut modifier. Si l'utilisateur dispose d'un accès à WorldClient, il peut également se connecter à WebAdmin depuis le menu options avancées de WorldClient.

Si l'utilisateur dispose d'une permission d'administrateur global ou de domaine (définie dans l'onglet Options 328) il peut accéder aux options de configuration.

WebAdmin - L'utilisateur est autorisé à modifier

Le nom réel
En activant cette option, l'utilisateur pourra modifier la valeur *Prénom et nom*.

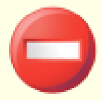
La boîte aux lettres
Autorise l'utilisateur à modifier le nom de sa boîte aux lettres.



Le nom de la boîte est équivalent à l'adresse e-mail. Par conséquent, si l'utilisateur la modifie, les messages envoyés à l'ancienne adresse risquent d'être rejetés ou supprimés.

Le mot de passe
Activez cette option si vous souhaitez autoriser l'utilisateur à modifier son mot de passe.

L'emplacement du dossier de courrier
Activez cette option si vous souhaitez autoriser l'utilisateur à modifier son Répertoire de messages 303.



Faites attention lorsque vous accordez cette autorisation aux utilisateurs. En donnant la possibilité aux utilisateurs de modifier leur répertoire de messages, il est possible que vous leur donniez accès à tous les répertoires sur votre système.

L'adresse de transfert
Lorsque cette option est activée, l'utilisateur peut modifier les paramètres de

transfert 313.

Le transfert avancé
Lorsque cette option est activée, l'utilisateur peut modifier ses paramètres de transfert avancés.

Les filtres IMAP
Utilisez cette option pour permettre aux utilisateurs de créer et de gérer leurs propres filtres de courrier 307. Cette fonctionnalité n'est disponible que dans MDaemon PRO.

L'option Ce compte est privé
Permet à l'utilisateur d'activer l'option Ce compte est privé se trouvant dans l'onglet Options 328 de l'Éditeur de compte.

Les restrictions
Cochez cette case pour autoriser l'utilisateur à modifier les options de l'onglet Restrictions 314.

Les quotas
Activez cette option si vous souhaitez autoriser le compte à modifier ses paramètres de quota 317.

Les paramètres MultiPOP
Cochez cette case si vous souhaitez que l'utilisateur puisse ajouter des entrées et activer/désactiver la collecte MultiPOP 320.

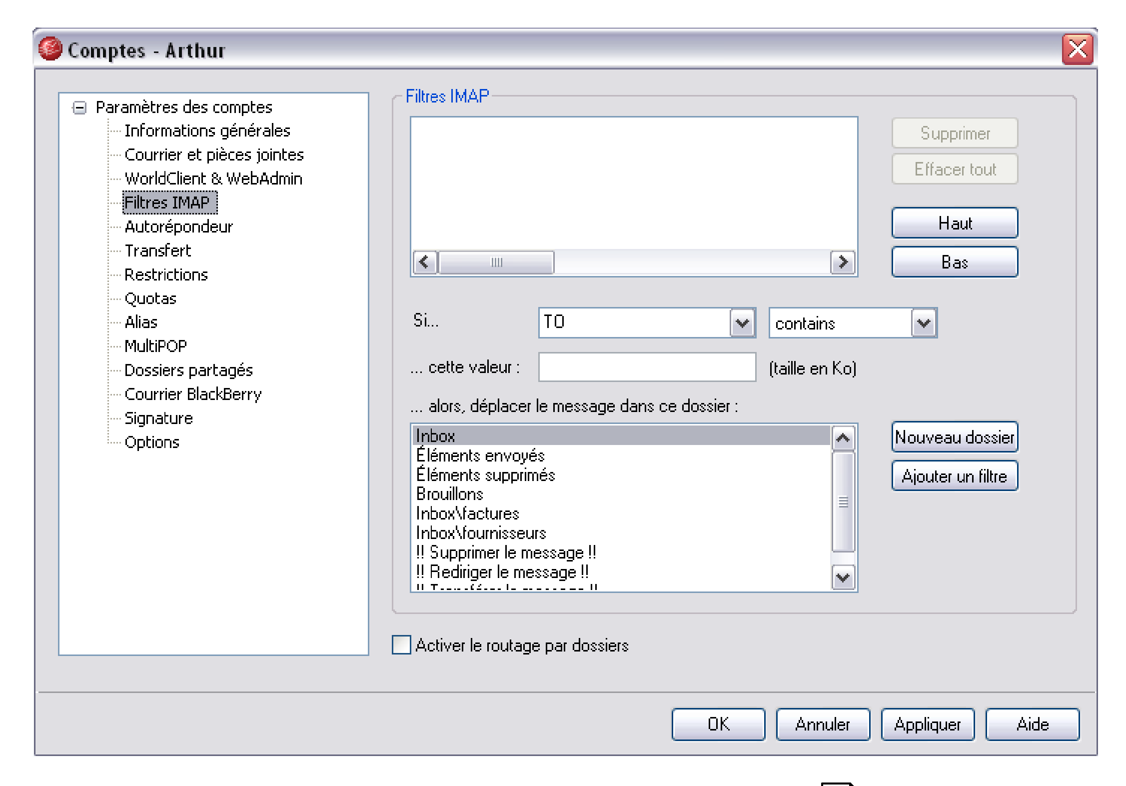
L'autorépondeur
Activez cette option si vous voulez que l'utilisateur puisse ajouter, modifier ou supprimer des autorépondeurs 310 pour son compte.

Les modifications par e-mail
Activez cette option si vous souhaitez que l'utilisateur puisse modifier les paramètres de son compte en envoyant des e-mails spécialement formatés 452.

La gestion des pièces jointes
Activez cette option si vous souhaitez que l'utilisateur puisse modifier les options de gestion des pièces jointes se trouvant dans l'onglet Courrier et pièces jointes 303 de l'Éditeur de compte.

Appliquer les paramètres par défaut
Cliquez sur ce bouton pour rétablir les valeurs par défaut figurant dans Comptes » Paramètres des comptes » Modèle de compte » WorldClient & WebAdmin 335.

5.1.1.4 Filtres IMAP



Avec MDaemon, le courrier des utilisateurs IMAP et WorldClient[106] peut être automatiquement dirigé vers des dossiers spécifiques sur le serveur. Tout comme avec le Filtre de contenu[178], MDaemon examine les en-têtes de chaque message et les compare aux filtres. Lorsqu'un message pour le détenteur du compte correspond à un des filtres, MDaemon le déplace vers le dossier indiqué dans ce filtre. Cette méthode est bien plus efficace (à la fois pour le client et le serveur) que de tenter de filtrer les messages sur chaque client, et comme certains clients IMAP ne prennent même pas en charge les filtres ou le filtrage de messages, les filtres de courrier leur fournissent cette fonctionnalité.

Les administrateurs peuvent créer des filtres à l'aide des options de cette fenêtre (ou depuis WebAdmin)[129]. Cependant, il est également possible d'accorder aux utilisateurs le droit de configurer eux-mêmes les filtres (voir WorldClient & WebAdmin)[304].

Règles IMAP

Dans cette zone s'affiche la liste de tous les filtres qui ont été créés pour le compte de l'utilisateur. Les filtres sont traités dans l'ordre de la liste jusqu'à ce qu'une correspondance soit trouvée. Par conséquent, dès qu'un message correspond à un des filtres, il est déplacé vers le dossier indiqué dans ce filtre et le l'application des filtres s'arrête alors. Utilisez les boutons Haut et Bas pour déplacer les filtres dans la liste.

Supprimer
Pour supprimer un filtre de la liste, sélectionnez-le et cliquez sur ce bouton.

Effacer tout
En cliquant sur ce bouton, vous supprimez tous les filtres de l'utilisateur.

Haut
Sélectionnez un filtre, puis cliquez sur ce bouton pour le déplacer vers le haut de la liste.

Bas
Sélectionnez un filtre, puis cliquez sur ce bouton pour le déplacer vers le bas de la liste.

Si la taille/l'en-tête du message
Sélectionnez *Message Size* ou le nom d'un en-tête dans le menu déroulant, ou bien saisissez le nom d'un en-tête. Si vous avez sélectionné un en-tête, MDaemon analyse cet en-tête dans tous les messages entrants et recherche la valeur indiquée dans le champ cette valeur ci-dessus. Ensuite, en fonction du type de comparaison faite, il déterminera les messages à déplacer dans le dossier indiqué par le filtre.

Liste de conditions
Il s'agit du type de comparaison qui sera faite lorsque des en-têtes ou la taille d'un message sont comparés aux filtres. MDaemon vérifie dans l'en-tête indiqué le texte contenu dans le champ cette valeur, puis procède en fonction du paramètre de cette commande—est-ce que le texte entier de l'en-tête correspond exactement, ne correspond pas exactement, ne le contient pas du tout, commence par lui, etc.

...cette valeur
Entrez le texte que vous souhaitez que MDaemon recherche lorsqu'il examine l'en-tête de message que vous avez indiqué pour cette règle. Si vous créez une règle en fonction de la taille du message, indiquez la valeur en Ko.

...alors déplacer le message dans le dossier
Après avoir indiqué les différents paramètres pour ce filtre, cliquez sur le dossier dans lequel vous souhaitez que les messages correspondant à cette règle soient déplacés, puis cliquez sur le bouton *Ajouter un filtre* pour le créer. Cette liste contient également trois entrées spécifiques :

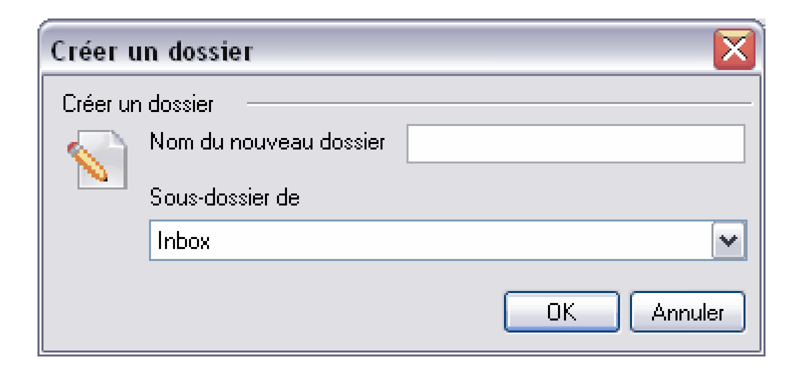
!! Supprimer le message!! – les messages correspondant aux conditions du filtre seront supprimés.

!! Rediriger le message !! – redirige le message entrant vers une autre adresse e-mail tel qu'il a été reçu (aucune modification n'est apportée au corps ou aux en-têtes). Le seul élément qui change est le destinataire de l'enveloppe SMTP.

!! Transférer le message !! – transfère le message entrant à un nouveau destinataire en introduisant un nouveau message dans le flux de courrier (en reprenant l'en-tête Subject et le corps du message d'origine).

Nouveau dossier
Cliquez sur ce bouton pour créer un nouveau dossier. La boîte de dialogue Créer un

dossier s'ouvre et vous pouvez indiquer un nom pour le dossier. Si vous voulez entrer un sous-dossier ou un dossier existant, sélectionnez-le dans la liste déroulante.



Ajouter un filtre
Lorsque vous avez choisi tous les paramètres du nouveau filtre, cliquez sur ce bouton pour l'ajouter à la liste..

Routage par dossiers

Ce système permet d'inclure le nom d'un dossier dans une adresse e-mail. Les réponses ou les messages envoyés à cette adresse seront automatiquement dirigés dans le dossier correspondant, sans devoir créer de filtre. Ainsi, les messages adressés à frank+mondossier@altn.com sont directement reçus dans le dossier "mondossier" de frank@altn.com (à condition évidemment que ce dossier existe). Si le nom du dossier contient un espace, il doit être remplacé par le caractère "_".

Par exemple, si frank.thomas@exemple.com possède un dossier appelé "Photos," le courrier adressé à "frank.thomas+Photos@exemple.com" sera routé automatiquement dans ce dossier. Il est possible de désigner des sous-dossiers en ajoutant le caractère "+". Ainsi, si le dossier "Photos" de Frank contient un sous-dossier "Vacances 2010", les messages envoyés à "frank. thomas+Photos+Vacances_2010@exemple.com" iront automatiquement dans le dossier \Photos\Vacances 2010\" de Frank.

Cette fonctionnalité utilisant le caractère "+", elle ne peut pas être utilisée si le nom de la boîte aux lettres contient ce caractère. De plus, il n'est pas possible d'utiliser des alias avec le routage par dossiers, mais vous pouvez créer un alias correspondant à la syntaxe complète. Par exemple : "alias+dossier@exemple.com" n'est pas valide, mais "alias@exemple.com" peut être utilisé pour remplacer "frank. thomas+dossier@exemple.com".

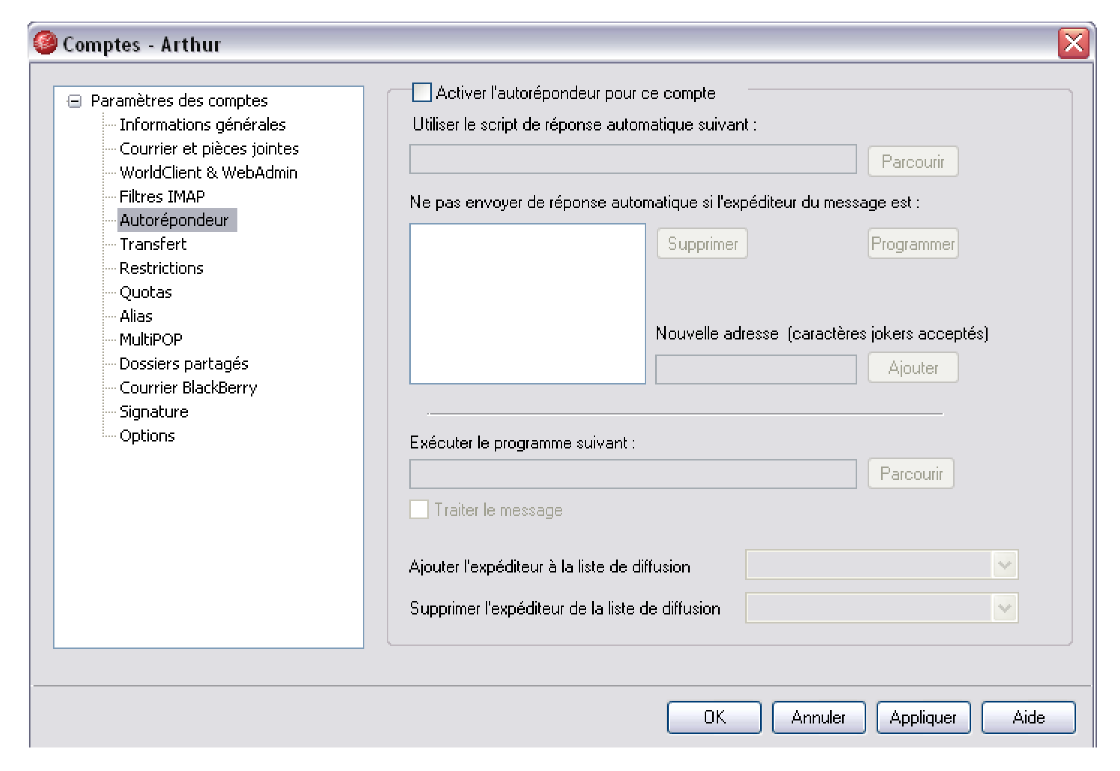
Afin d'éviter les attaques et piratages, le nom de dossier IMAP indiqué dans l'adresse doit absolument être valide. Si le nom de dossier indiqué dans l'adresse n'existe pas, l'adresse est considérée comme inconnue et le message est traité en conséquence. Par exemple, si un message est envoyé à "frank+photos@exemple.com" et que frank@exemple.com ne possède pas de dossier "photos", le message est considéré comme adressé à un utilisateur inconnu.

Activer le routage par dossiers
Cochez cette case pour autoriser le routage par dossiers pour ce compte.

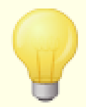


Cette fonctionnalité est désactivée par défaut pour tous les comptes. De plus, il est possible de la désactiver globalement dans l'onglet Divers 167 de la boîte de dialogue Préférences. Dans ce cas, cette fonctionnalité n'est accessible pour aucun compte, quels que soient ses paramètres.

5.1.1.5 Autorépondeur



Les autorépondeurs sont des outils permettant de déclencher des événements spécifiques lorsqu'un message entrant est reçu (exécuter un programme, ajouter l'expéditeur à une liste de diffusion, envoyer une réponse automatique...). Les autorépondeurs sont le plus couramment utilisés pour envoyer une réponse automatique indiquant par exemple que le destinataire est absent, en congés, etc. Les utilisateurs disposant de droits d'accès à WorldClient 106 ou WebAdmin 129 disposent d'options leur permettant de choisir le contenu de la réponse automatique et définir les dates d'application de l'autorépondeur. Enfin, les messages de réponse automatique sont basés sur des fichiers de script (`*.RSP`) supportant un grand nombre de macros afin de personnaliser le message.



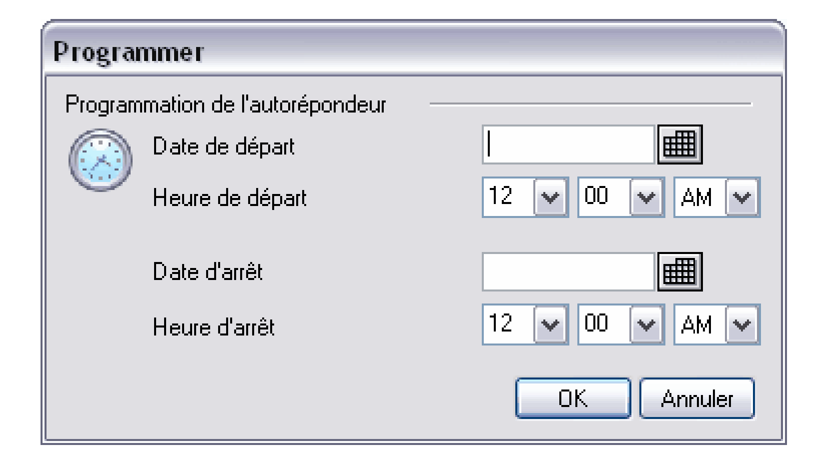
Les réponses automatiques sont toujours honorées lorsque le message déclencheur provient d'une source distante. Pour les

messages locaux, le déclenchement de l'autorépondeur dépend de l'option *L'autorépondeur est déclenché par le courrier local*, située dans Autorépondeur » Options 342.

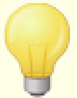
Activer l'autorépondeur pour ce compte
Cochez cette case pour activer un autorépondeur pour ce compte. Pour plus d'informations sur les autorépondeurs, voir : Autorépondeurs 339.

Utiliser le script de réponse automatique suivant
Ce champ indique le chemin complet et le nom de fichier du fichier de réponse (*.RSP) qui sera traité et distribué à l'expéditeur du message. Le fichier doit d'abord passer dans le mécanisme de filtrage associé aux fichiers MBF. Chaque chaîne de modèle pouvant être utilisée dans un fichier MBF pourra également être utilisée dans un fichier de réponse automatique. Voir création de scripts de réponse automatique 343.

Programmer
Cliquez sur ce bouton pour ouvrir la boîte de dialogue Programmer dans laquelle vous pouvez définir une date de début et de fin pour l'activation de l'autorépondeur. Pour que l'autorépondeur soit toujours actif, laissez le champ correspondant à la programmation vide.



Ne pas envoyer de réponse automatique si l'expéditeur du message est :
Vous pouvez indiquer dans cette zone les adresses à exclure des réponses de l'autorépondeur.



Parfois, les messages de réponse automatique sont envoyés à une adresse qui retourne elle-même une réponse. Cela peut provoquer un effet "ping-pong" par lequel les messages feraient continuellement la navette entre les deux serveurs. Vous pouvez utiliser cette fonctionnalité pour éviter que l'autorépondeur de MDaemon n'envoie des réponses à une ou plusieurs adresses en les saisissant dans cette zone. Une option située dans Autorépondeurs » Options 342, permet

également de limiter l'envoi de réponses automatiques à une réponse par expéditeur et par jour.

Supprimer
Pour supprimer une entrée de la liste des adresses à exclure, sélectionnez-la et cliquez sur ce bouton.

Nouvelle adresse (caractères jokers acceptés)
Si vous souhaitez ajouter une adresse à la liste des adresses exclues, saisissez-la ici, puis cliquez sur le bouton *Ajouter*.

Exécuter un programme

Exécuter le programme suivant :
Ce champ indique le chemin complet et le nom de fichier d'un programme qui sera lancé lorsque de nouveaux messages arrivent dans la boîte aux lettres indiquée. Assurez-vous que ce traitement se termine correctement et peut être exécuté sans surveillance. Des paramètres de ligne de commande optionnels peuvent être entrés immédiatement après le chemin exécutable si vous le souhaitez.

Traiter le message
Sélectionnez cette option et l'exécutable indiqué dans le champ *Exécuter le programme suivant* passera le nom du message déclencheur comme premier paramètre de ligne de commande disponible. Le temps que le nom du message soit traité par programme indiqué, le fichier MBF du compte aura déjà été appliqué. Cela est utile puisque qu'en appliquant un MBF, le message peut être reformaté dans une structure cohérente sans tenir compte de la source du message d'origine. Lorsque l'autorépondeur est configuré sur un compte qui transfère du courrier vers un autre emplacement et ne conserve pas une copie locale dans sa propre boîte aux lettres (voir Transfert 313), cette fonction est alors désactivée.



Par défaut, MDaemon place le nom du fichier de message comme dernier paramètre dans la ligne de commande. Vous pouvez éviter ce comportement à l'aide de la macro $MESSAGE$. Utilisez cette macro là où le nom du fichier de message doit être placé. Cela permet une plus grande flexibilité dans l'utilisation de cette fonctionnalité puisqu'une ligne de commande complexe du type logmail /e /j / message=$MESSAGE$ /q est possible.

Listes de diffusion

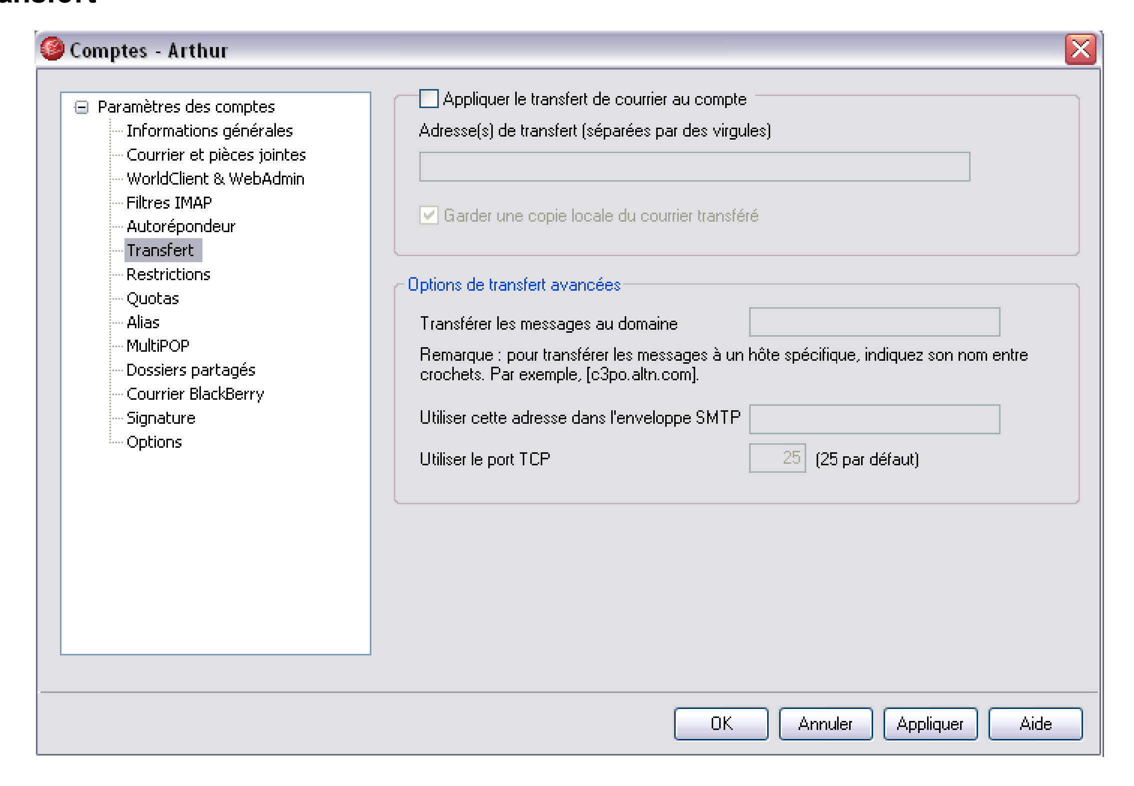
Ajouter l'expéditeur à la liste de diffusion
Si une liste de diffusion est indiquée dans ce champ, l'expéditeur du message est alors ajouté automatiquement à cette liste de diffusion. Cette fonctionnalité est particulièrement pratique pour créer des listes automatiquement.

Supprimer l'expéditeur de la liste de diffusion
Si une liste de diffusion est indiquée dans ce champ, l'expéditeur du message est alors supprimé automatiquement de la liste de diffusion indiquée.

Voir également :

Autorépondeurs » Comptes 339
Autorépondeurs » Exceptions 341
Autorépondeurs » Options 342
Création de scripts de réponse automatique 343

5.1.1.6 Transfert



Options de transfert

Appliquer le transfert de courrier au compte
Activez cette option si vous souhaitez que le courrier adressé à ce compte soit transféré à l'adresse indiquée dans le champ *Adresse(s) de transfert*. Les utilisateurs disposant de droits d'accès à WorldClient 106 ou WebAdmin 129 peuvent configurer eux-mêmes le transfert du courrier.

Adresse(s) de transfert (séparées par des virgules)
Ce champ vous permet d'indiquer une adresse à laquelle les copies de tous les messages entrants destinés à ce compte seront automatiquement transférés

lorsqu'ils arrivent sur le serveur et sont distribués dans le répertoire de courrier local de ce compte. Si vous en indiquez plusieurs, séparez-les par des virgules.

Garder une copie locale du message transféré
Par défaut une copie de chaque message transféré est envoyée au compte.

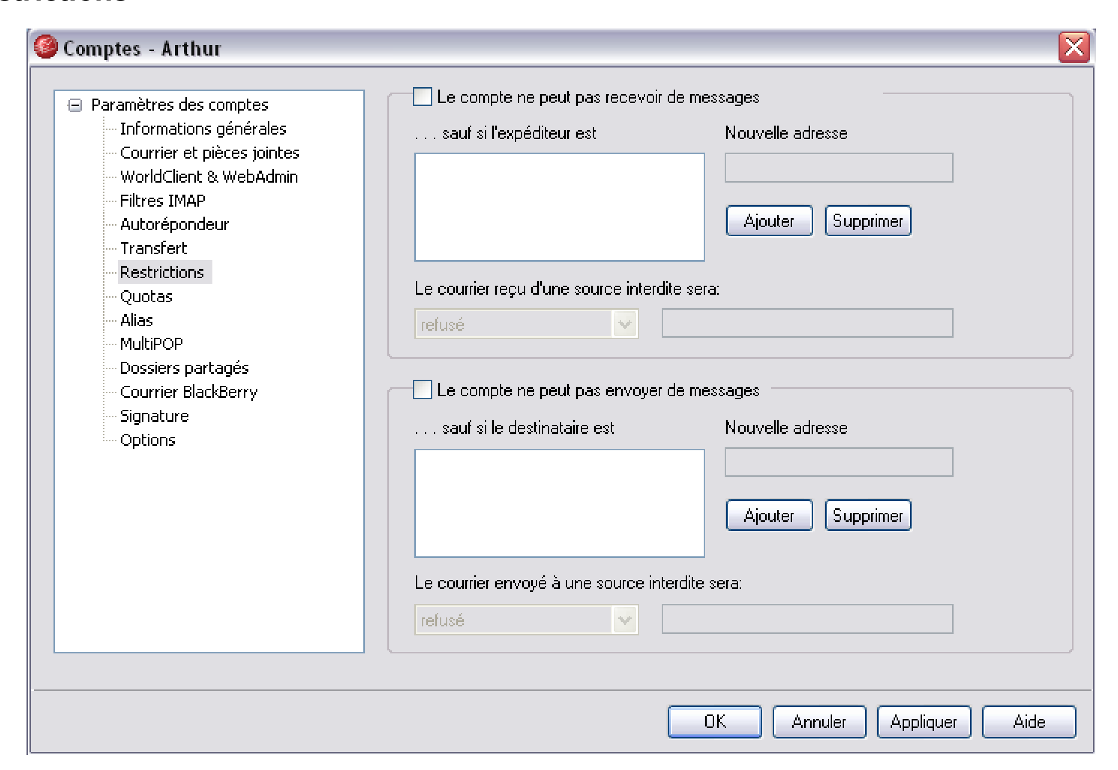
Options de transfert avancées

Transférer les messages au domaine
Si vous souhaitez diriger les messages transférés aux serveurs MX d'un domaine spécifique, indiquez ici le nom de ce domaine. Si vous souhaitez les diriger vers un hôte spécifique, saisissez son nom entre parenthèses (par ex. : [hote1.exemple.com]).

Utiliser cette adresse dans l'enveloppe SMTP
Si une adresse est indiquée ici, elle sera utilisée dans la commande SMTP "Mail From:" lors de l'établissement d'une communication avec l'hôte. Normalement, l'expéditeur du message est utilisé dans cette portion de l'enveloppe SMTP. Si vous devez utiliser une commande "Mail From:" vide (du type MAIL FROM <>), saisissez alors "[trash]" dans ce champ.

Utiliser le port TCP
MDaemon envoie les messages transférés sur le port TCP indiqué dans ce champ.

5.1.1.7 Restrictions



Ces options permettent de contrôler si le compte peut ou non envoyer et recevoir du courrier à ou depuis des domaines non locaux. Le Modèle de compte 330 contient une option permettant d'appliquer cette restriction à tous les comptes par défaut.

Courrier entrant

Le compte ne peut pas recevoir de messages
Activez cette option si vous voulez que le compte ne puisse pas recevoir de messages de domaines non locaux.

...sauf si l'expéditeur est
Les adresses indiquées dans cette zone sont des exceptions aux restrictions du courrier entrant. Les caractères jokers sont autorisés. Par exemple, si vous indiquez "*@altn.com" comme exception, tous les messages entrants provenant d'une adresse de altn.com seront acceptés et distribués à ce compte.

Nouvelle adresse
Si vous souhaitez ajouter une exception dans la liste, saisissez cette adresse ici et cliquez sur le bouton *Ajouter*.

Ajouter
Après avoir saisi une adresse, cliquez sur ce bouton pour l'ajouter à la liste des exceptions.

Supprimer
Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur ce bouton.

Le courrier reçu d'une source interdite sera...
Sélectionnez l'action à effectuer lorsqu'un message provenant d'un domaine non local est reçu :

refusé – Les messages interdits seront refusés par MDaemon.

renvoyé à l'expéditeur – Les messages provenant d'adresses interdites seront retournés à l'expéditeur.

envoyé au postmaster – Les messages interdits seront acceptés mais distribués au postmaster et non à ce compte.

envoyé à... – Les messages interdits seront acceptés mais distribués à l'adresse indiquée.

Courrier sortant

Le compte ne peut pas envoyer de messages
Activez cette option si vous souhaitez que le compte ne puisse pas envoyer de messages à des domaines non locaux.

...sauf si le destinataire est
Les adresses indiquées dans cette zone sont des exceptions aux restrictions du courrier sortant. Les caractères jokers sont autorisés. Par exemple, si vous indiquez "*@altn.com" comme exception, tous les messages entrants provenant

d'une adresse de altn.com seront acceptés et distribués à ce compte.

Nouvelle adresse
Si vous souhaitez ajouter une exception dans la liste, saisissez cette adresse ici et cliquez sur le bouton *Ajouter*.

Ajouter
Après avoir saisi une adresse, cliquez sur ce bouton pour l'ajouter à la liste des exceptions.

Supprimer
Pour supprimer une adresse de la liste, sélectionnez-la et cliquez sur ce bouton.

Le courrier envoyé à une source interdite sera...
Sélectionnez l'action à effectuer lorsqu'un message est envoyé à un domaine non local :

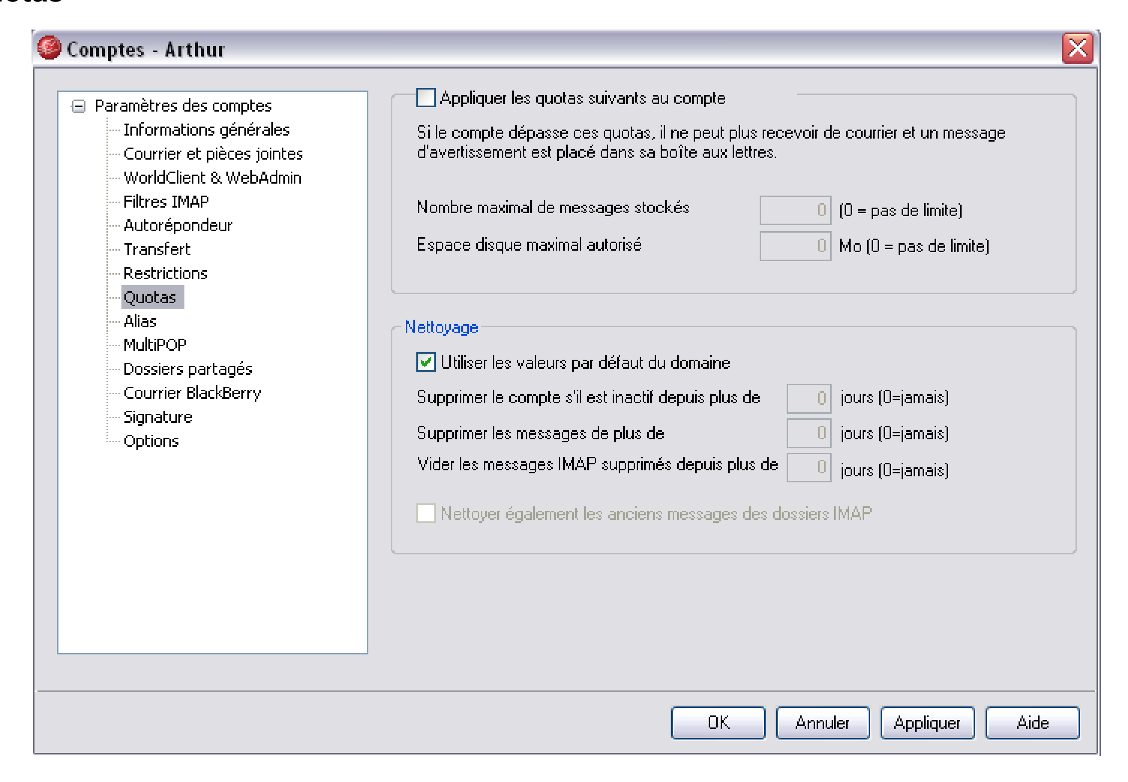
refusé – Les messages interdits seront refusés par MDaemon.

renvoyé à l'expéditeur – Les messages provenant d'adresses interdites seront retournés à l'expéditeur.

envoyé au postmaster – Les messages interdits seront acceptés mais distribués au postmaster et non au destinataire d'origine.

envoyé à... – Les messages interdits seront acceptés mais distribués à l'adresse indiquée.

5.1.1.8 Quotas



Options de quotas

Appliquer les quotas suivants au compte
Activez cette option si vous souhaitez contrôler le nombre maximal de messages autorisés sur le compte et le total maximal d'espace disque (en Ko) que le compte peut utiliser (cela inclut toutes les pièces jointes décodées dans le Répertoire de fichiers du compte). Si la réception d'un message entraîne le dépassement des quotas pour le nombre de messages ou l'espace disque, le message est refusé et un avertissement est placé dans le répertoire de courrier de l'utilisateur. Si une collecte MultiPOP dépasse la limite maximum du compte, un message d'avertissement similaire est émis et les entrées MultiPOP du compte sont automatiquement éteintes (mais ne sont pas retirées de la base de données).



Il est possible d'envoyer un message d'avertissement lorsqu'un certain pourcentage du quota est atteint, à l'aide de l'option située dans "Comptes » Paramètres des comptes » Quotas 338". Ce message contient le nombre de messages et l'espace utilisés, les quantités autorisées, ainsi que l'espace restant. De plus, si un message d'avertissement se trouve déjà dans la boîte aux lettres, il est remplacé par le nouveau.

Nombre maximal de messages stockés
Indiquez ici le nombre maximal de messages pouvant être stockés pour ce compte ("0" = pas de limite).

Espace disque maximal autorisé
Indiquez ici la quantité maximale d'espace disque pouvant être utilisé par le compte (y compris les pièces jointes enregistrées dans le dossier `\Files`). ("0" = pas de limite.)

Nettoyage

Les options de cette section servent à indiquer si le compte doit être supprimé par MDaemon lorsqu'il est inactif. Vous pouvez également indiquer si les anciens messages appartenant à ce compte sont ou non supprimés après un certain laps de temps. Chaque jour à minuit, MDaemon retire tous les messages ayant dépassé les limites de temps, ou il supprime complètement le compte s'il a atteint la limite d'inactivité.

Utiliser les valeurs par défaut du domaine
Les paramètres de nettoyage du domaine se trouvent dans : Domaine/serveurs par défaut » Nettoyage 54 ou Domaines supplémentaires 103. Si vous souhaitez utiliser des paramètres spécifiques pour ce compte, décochez cette option et remplissez les champs ci-dessous.

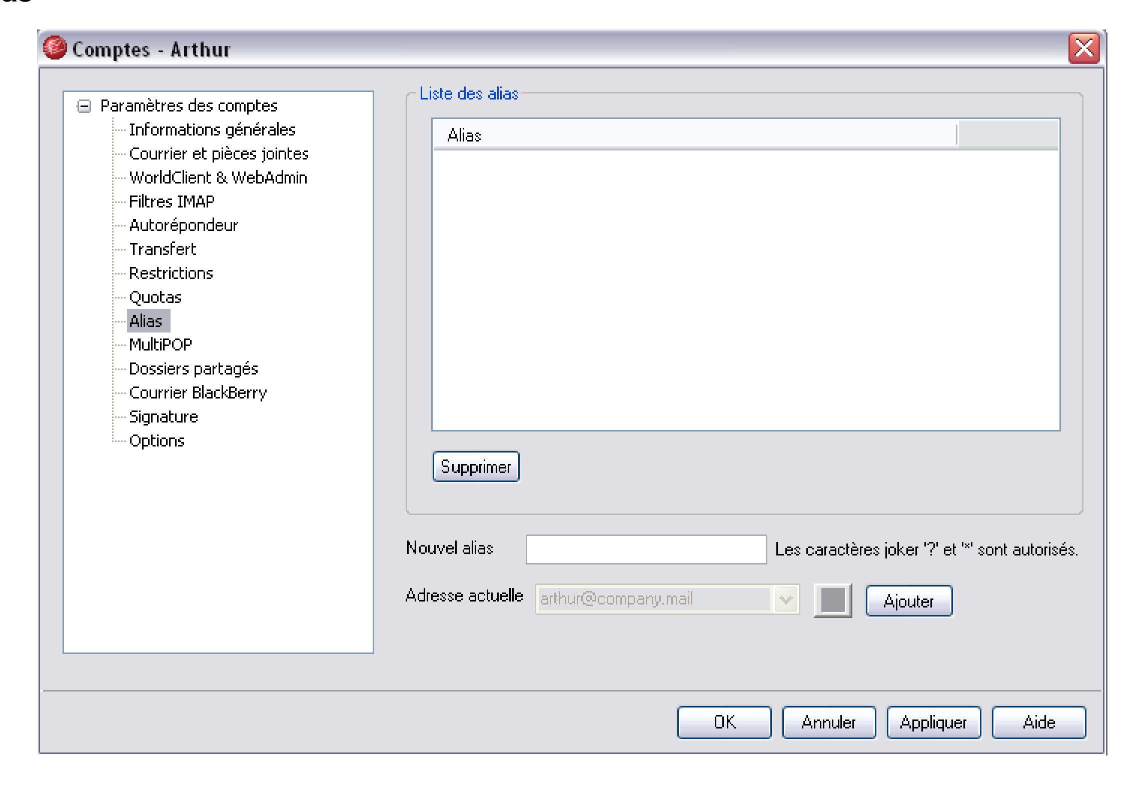
Supprimer le compte si inactif depuis plus de XX jours (0 = jamais)
Nombre de jours d'inactivité autorisés avant la suppression automatique du compte.

Supprimer les messages de plus de XX jours (0 = jamais)
La valeur indiquée dans cette commande correspond au nombre de jours qu'un message donné peut rester dans la boîte aux lettres du compte avant d'être supprimé automatiquement par MDaemon.

Vider les messages IMAP supprimés depuis plus de [XX] jours (0 = jamais)
Indiquez pendant combien de jours les messages IMAP marqués comme supprimés sont conservés dans les dossiers de l'utilisateur.

Nettoyer également les anciens messages des dossiers IMAP
Cochez cette case si vous souhaitez que l'option *Supprimer les messages de plus de...* s'applique également aux messages des dossiers IMAP. Lorsque cette option est désactivée, les messages contenus dans ces dossiers ne seront pas supprimés en raison de leur ancienneté.

5.1.1.9 Alias



Affiche la liste des alias 347 associés à ce compte, et permet d'en ajouter ou d'en supprimer.

Supprimer un alias

Pour supprimer un alias, sélectionnez-le et cliquez sur le bouton **Supprimer**.

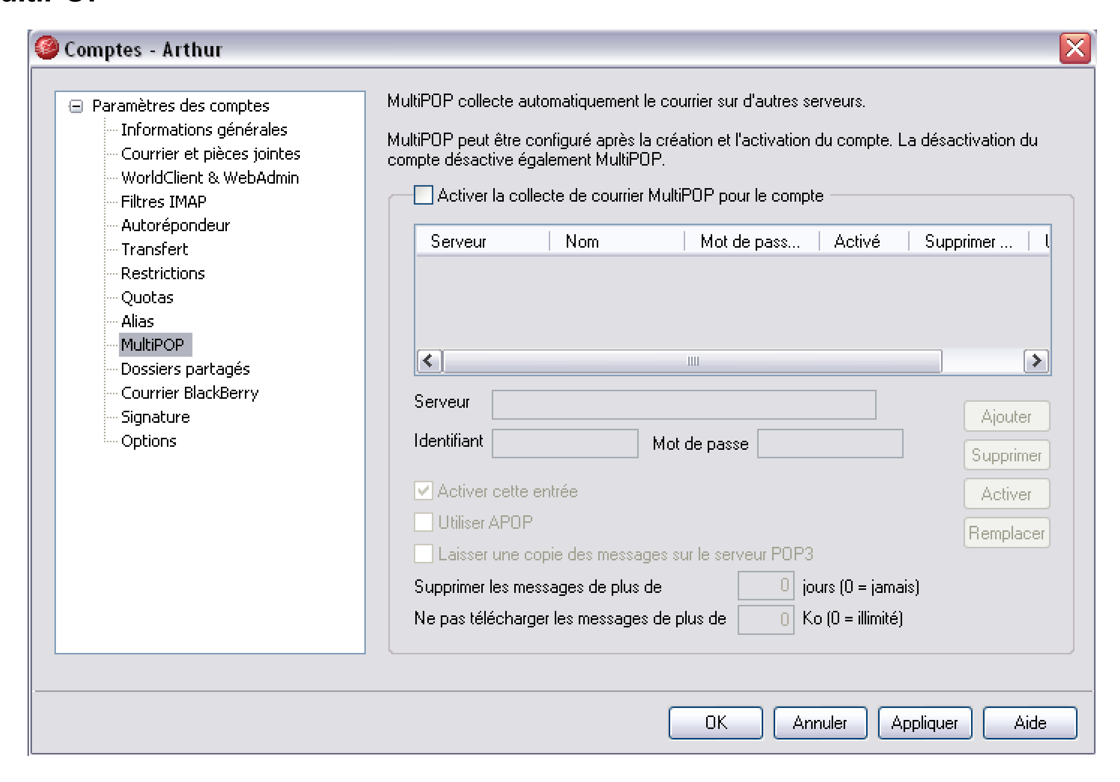
Ajouter un alias

Pour ajouter un alias, saisissez l'adresse choisie dans le champ *Nouvel alias* puis cliquez sur le bouton **Ajouter**. Les caractères joker "?" et "*" sont autorisés.

Voir également :

Alias d'adresses 347

5.1.1.10 MultiPOP



La fonctionnalité MultiPOP permet d'indiquer un nombre illimité de combinaisons hôte/ utilisateur/mot de passe POP pour la collecte de messages depuis plusieurs sources. Cela est utile pour vos utilisateurs qui disposent de comptes de messagerie sur plusieurs serveurs mais qui préfèrent collecter et rassembler tout leur courrier au même endroit. Avant d'être placé dans la boîte aux lettres de l'utilisateur, le courrier collecté par MultiPOP est d'abord placé dans la file d'attente locale pour être traité de la même façon que le courrier avec autorépondeurs ou celui auquel s'appliquent le Filtre de contenu. Les options de programmation de la collecte MultiPOP se trouvent dans : Configuration » Programmation d'événements » Distribution du courrier » Collecte MultiPOP 146.

Activer la collecte de courrier MultiPOP pour le compte
Ce paramètre doit être activé pour que le traitement MultiPOP ait lieu pour le compte.

Listes des hôtes
Listes des hôtes MultiPOP configurés pour ce compte.

Création ou modification d'un hôte

Serveur
Nom du serveur POP3 à partir duquel vous souhaitez collecter le courrier.

Identifiant
Entrez le nom d'utilisateur ou l'identifiant POP3 qui permet d'accéder au serveur indiqué.

Mot de passe
Entrez le mot de passe POP3 ou APOP servant à accéder au compte de messagerie sur le serveur indiqué.

Utiliser APOP
Activez cette option si vous voulez que l'entrée MultiPOP utilise la méthode d'authentification APOP lors du retrait de courrier depuis l'hôte correspondant.

Laisser une copie des messages sur le serveur POP3
Activez cette option si vous voulez laisser une copie des messages collectés sur le serveur. Cela est utile lorsque vous prévoyez de retirer à nouveau ces messages plus tard depuis un autre emplacement.

Supprimer les messages de plus de [XX] jours (0 = jamais)
Nombre de jours pendant lesquels les messages sont conservés sur l'hôte MultiPOP avant d'être supprimés. Indiquez "0" si vous ne souhaitez pas supprimer les anciens messages.

Ne pas télécharger les messages de plus de X Ko (0 = illimité)
Entrez une valeur ici si vous voulez limiter la taille des messages à télécharger.

Ajouter
Après avoir rempi les champs ci-dessus, cliquez sur ce bouton pour ajouter l'hôte à la liste.

Supprimer
Pour supprimer un hôte de la liste, sélectionnez-le et cliquez sur ce bouton.

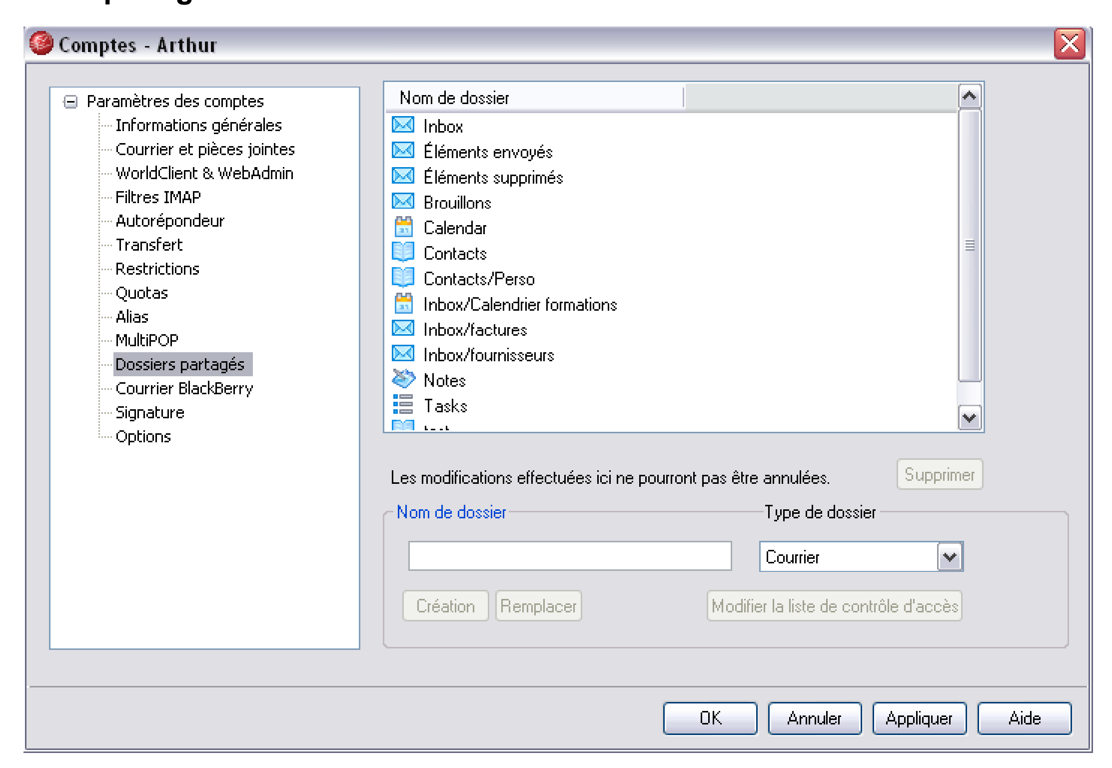
Activer/désactiver
En cliquant sur ce bouton, l'état des hôtes MultiPOP sélectionnés se modifie. Ce paramètre vous permet de décider si MDaemon collecte du courrier pour cet hôte ou l'ignore lorsqu'il effectue le traitement MultiPOP.

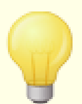
Remplacer
Lorsqu'une entrée est sélectionnée dans la liste, elle peut être modifiée. Après avoir effectué les modifications souhaitées, cliquez sur ce bouton pour les appliquer.

Voir également :

Programmation d'événements » Collecte MultiPOP 146

5.1.1.11 Dossiers partagés





Cet onglet n'est disponible que lorsque l'option *Activer les dossiers publics* est activée dans Configuration » Domaine/ serveurs par défaut » Dossiers publics et partagés 66.

Dossiers IMAP

Affiche tous les dossiers IMAP de l'utilisateur, dont l'accès peut être partagé avec d'autres utilisateurs ou groupes. Lors de la création du compte, cette partie est vide. Utilisez les options *Nom de dossier* et *Créer* (ou bien celles de l'onglet Filtres 307) pour ajouter un dossier. Le caractère utilisé pour séparer les noms de dossiers et sous-dossiers est "/".

Supprimer

Pour supprimer un dossier IMAP partagé de la liste, sélectionnez-le puis cliquez sur *Supprimer*.

Nom de dossier

Saisissez le nom du nouveau dossier puis cliquez sur *Créer*. Si vous souhaitez obtenir un sous-dossier pour l'un des dossiers de la liste, ajoutez le nom du parent au début ainsi que le caractère "/". Par exemple, si le dossier parent s'appelle "Mon dossier", le sous-dossier s'intitule "Mon dossier/Mon nouveau dossier".

Type de dossier

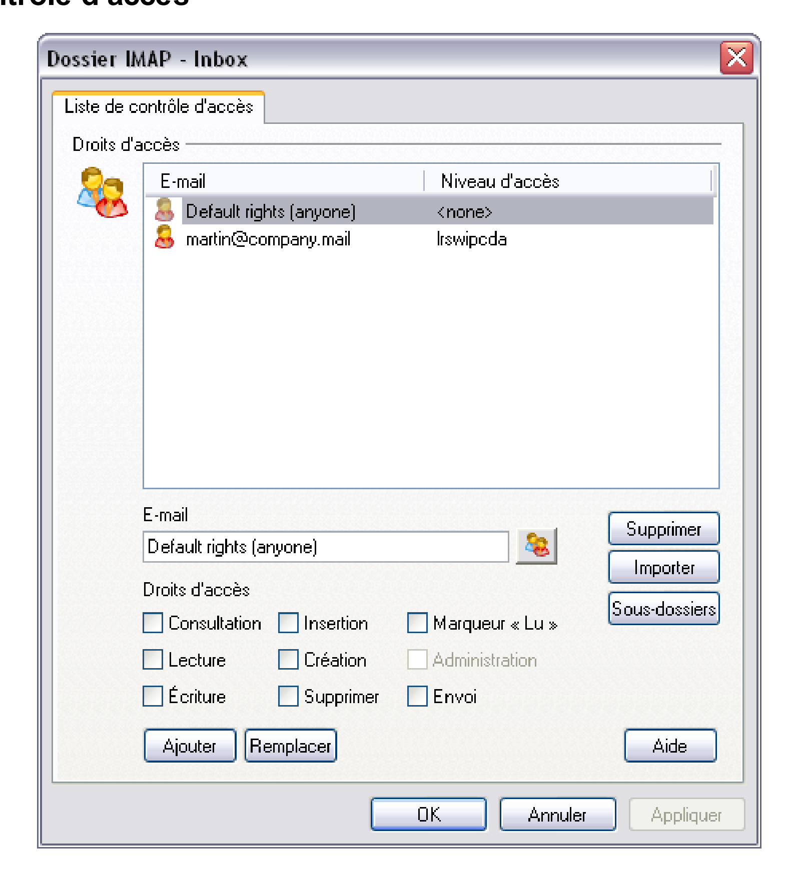
Sélectionnez le type de dossier à créer : Courrier, Calendrier, Contacts, etc.

Créer
Cliquez sur ce bouton pour ajouter le dossier à la liste.

Remplacer
Pour modifier un dossier partagé, cliquez sur son nom, effectuez les modifications, puis cliquez sur *Remplacer*.

Modifier la liste de contrôle d'accès
Cette option permet de choisir quels utilisateurs ou groupes ont accès au dossier, et de leur attribuer des permissions. Pour cela, sélectionnez un dossier, puis cliquez sur ce bouton pour ouvrir la Liste de contrôle d'accès323.

5.1.1.11.1 Liste de contrôle d'accès



Droits d'accès

Il est possible d'accorder l'accès à un dossier partagé, ainsi que des permissions à certains utilisateurs ou groupes. Pour cela, cliquez sur Dossiers partagés322 dans l'Editeur de compte, puis effectuez un double clic sur un dossier ou sélectionnez-le puis cliquez sur *Modifier la liste de contrôle d'accès*. Chaque entrée de la liste contient l'adresse e-mail d'un compte ainsi qu'une abréviation des droits d'accès qu'il possède.

E-mail
Indiquez le compte ou le groupe pour lequel vous souhaitez accorder l'accès à ce dossier ou bien cliquez sur l'icône pour le sélectionner. Choisissez ensuite les droits d'accès puis cliquez sur *Ajouter*.

Supprimer
Pour supprimer une entrée de la liste, sélectionnez-la puis cliquez sur ce bouton.

Importer
Cette fonctionnalité permet d'ajouter les membres d'une autre liste à celle-ci. Choisissez les droits que désirez accorder, cliquez sur *Importer*, puis double-cliquez sur la liste choisie : tous ses membres seront ajoutés.

Sous-dossiers
Sélectionnez un compte ou groupe et cliquez sur ce bouton si vous souhaitez appliquer les droits à tous les sous-dossiers du dossier sélectionné.

Droits d'accès

Choisissez les droits que vous souhaitez accorder, puis cliquez sur *Ajouter* pour une nouvelle entrée ou *Remplacer* pour une entrée déjà existante.

Consultation (l) – l'utilisateur peut voir le dossier dans la liste.

Lecture (r) – l'utilisateur peut ouvrir le dossier et afficher son contenu.

Écriture (w) – l'utilisateur peut changer les indicateurs de message du dossier.

Insertion (i) – l'utilisateur peut ajouter et copier des messages dans le dossier.

Création (c) - l'utilisateur peut créer des sous-dossiers.

Supprimer (d) – l'utilisateur peut supprimer des messages du dossier.

Marqueur lu (s) – l'utilisateur peut modifier le statut "lu".

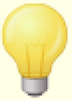
Administration (a) – l'utilisateur peut administrer la liste de contrôle d'accès du dossier.

Envoi (p) – l'utilisateur peut envoyer des messages directement dans le dossier (si les paramètres du dossier le permettent).

Ajouter
Après avoir choisi une adresse e-mail ou un groupe et déterminé les droits qui lui sont accordés, cliquez sur ce bouton pour l'ajouter à la liste.

Remplacer
Pour modifier une entrée de la liste de contrôle d'accès, sélectionnez-la, effectuez les modifications, puis cliquez sur *Remplacer*.

Aide
Affiche la liste des droits d'accès ainsi que leur définition.



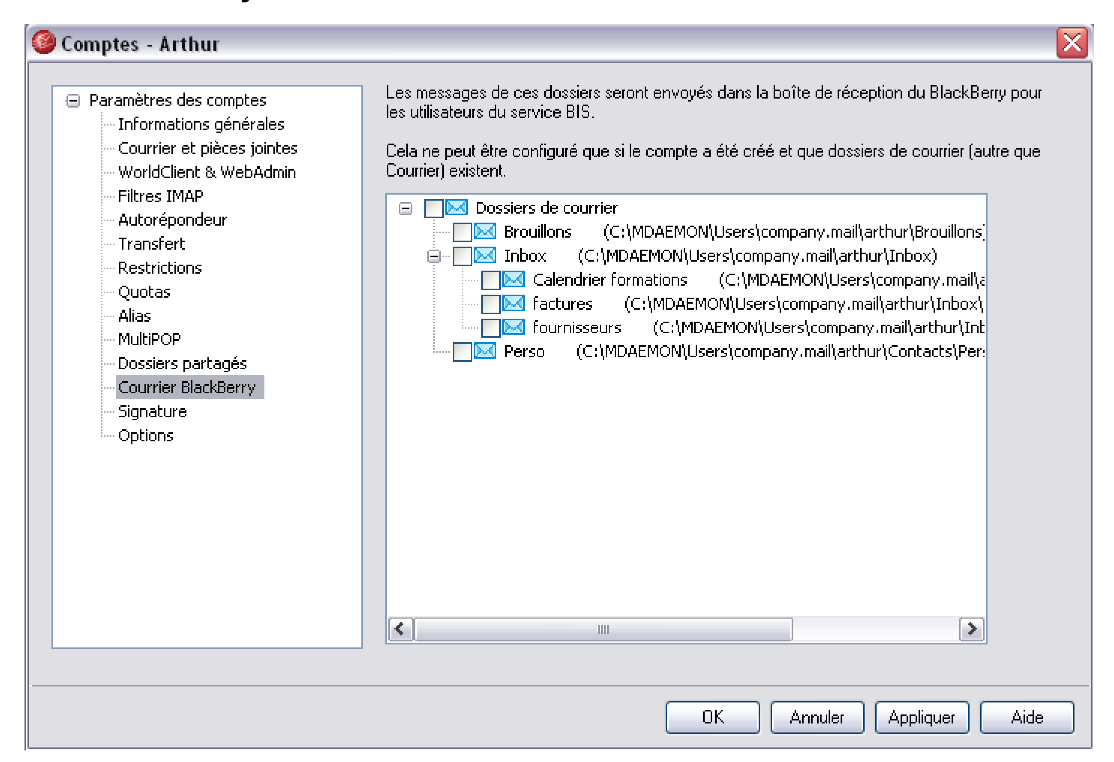
Les droits d'accès sont contrôlés grâce au support des listes de contrôle d'accès (ACL). Elles constituent une extension du protocole IMAP4 qui permet de créer une liste d'accès pour chacun de vos dossiers de messages IMAP, et accorde ainsi des droits d'accès à vos dossiers à d'autres utilisateurs qui possèdent également des comptes sur votre serveur de messagerie. Si votre client de messagerie n'est pas compatible avec les ACL, vous pouvez toujours définir ces autorisations à l'aide des commandes de cette boîte de dialogue.

Pour obtenir des informations complètes sur les ACL, consultez : http://www.rfc-editor.org/rfc/rfc2086.txt.

Voir également :

Éditeur de compte » Dossiers partagés 322
Dossiers publics et partagés 66
Liste des dossiers 68

5.1.1.12 Courrier BlackBerry



Si l'utilisateur utilise un smartphone BlackBerry pour collecter le courrier, vous pouvez

indiquer ici les dossiers IMAP pour lesquels vous souhaitez envoyer les messages reçus sur le Blackberry. En effet, BlackBerry Internet Service collecte uniquement le contenu de la boîte de réception, et non celui des autres dossiers du compte. Par conséquent, si l'utilisateur a créé des filtres IMAP 307 pour recevoir automatiquement les messages dans des dossiers spécifiques, ces messages ne sont pas collectés par BIS. Cette fenêtre permet d'envoyer les messages ainsi filtrés sur le BlackBerry. Attention, seuls les nouveaux messages reçus sont distribués, les anciens messages déjà présents dans ces dossiers ne sont pas envoyés sur le BlackBerry.



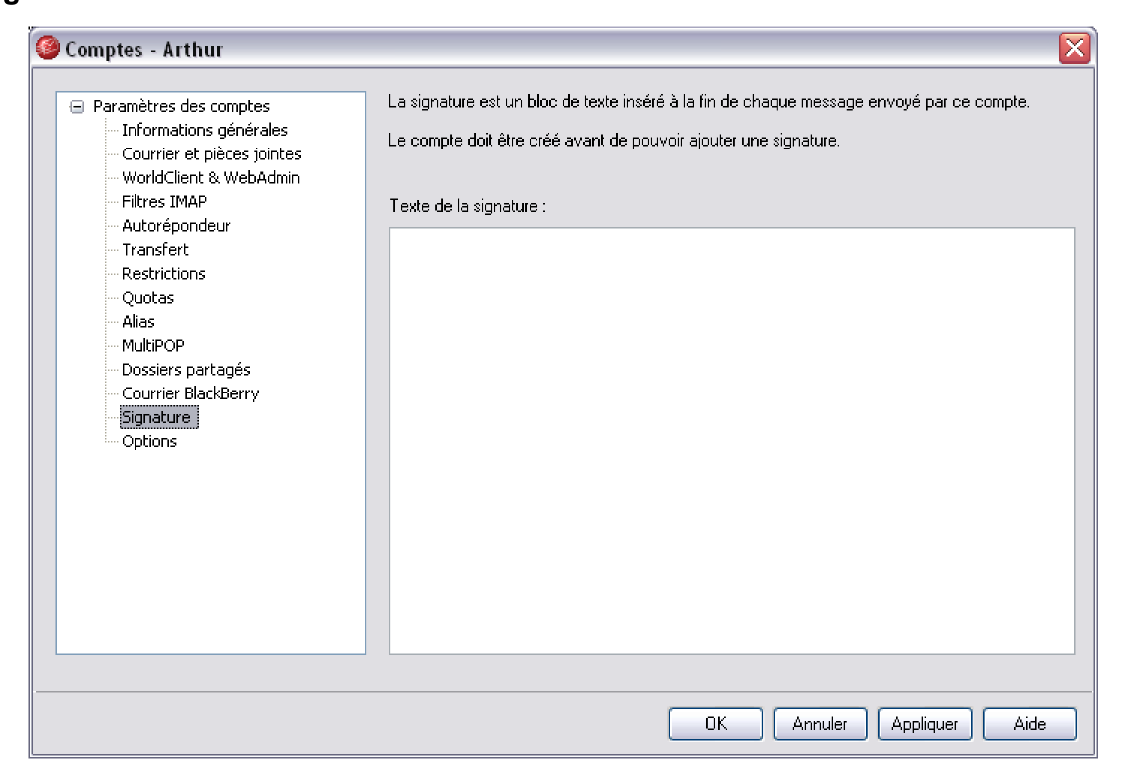
Ces messages restent dans leurs dossiers respectifs sur le serveur MDaemon et les dossiers ne sont pas créés sur le BlackBerry. Ils sont simplement envoyés sur le BlackBerry comme s'ils appartenaient au dossier de courrier.

La page Dossiers des options de WorldClient permet à l'utilisateur de sélectionner lui-même les dossiers de son choix (option *Envoyer vers BlackBerry*). Cette option n'est disponible que si vous avez activé "*Autoriser la sélection de dossiers autres que "Courrier"*" dans les paramètres d'intégration BlackBerry 155.

Voir également :

BlackBerry Internet Service 149

5.1.1.13 Signature

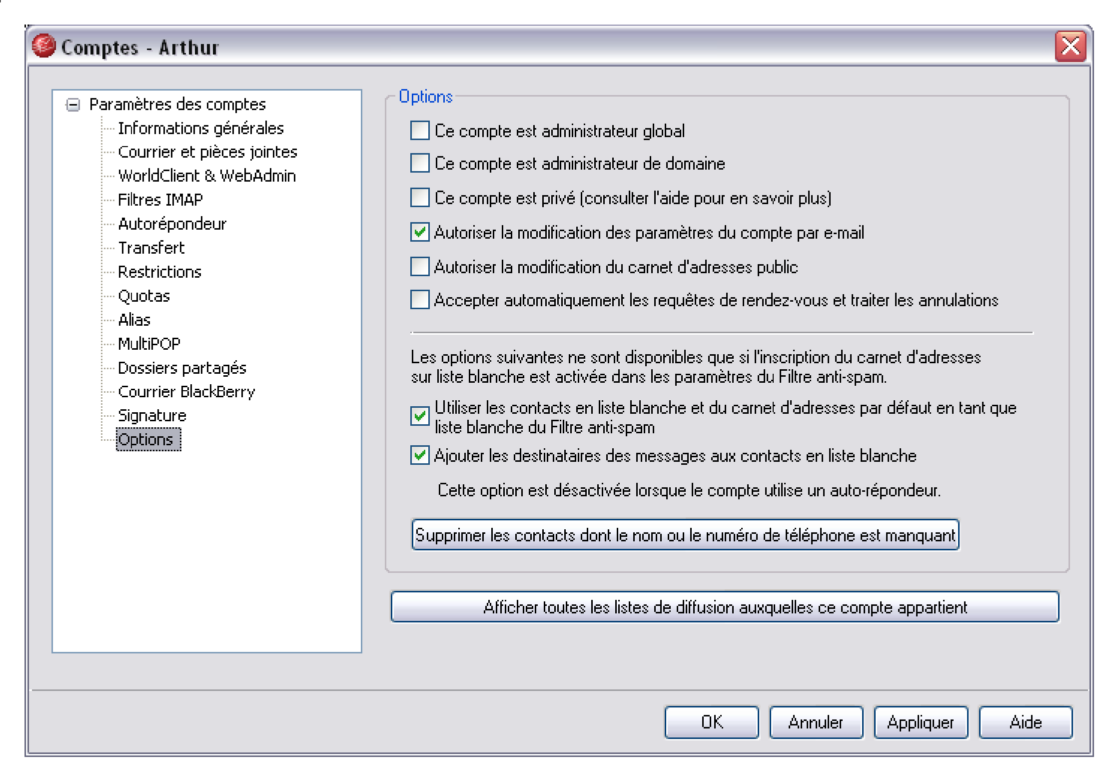


Texte de la signature

Cet onglet permet de définir une signature qui sera incluse à la fin de chaque message envoyé par le compte. Elle précède les autres signatures générées par d'autres options telles que la signature de WorldClient ou autres clients de messagerie, les signatures de domaine 64 et les pieds de page des listes de diffusion 392.

Les utilisateurs disposant de droits d'accès à WebAdmin 129 peuvent modifier leur signature en cliquant sur Mon comtpe » Signature dans WebAdmin.

5.1.1.14 Options



Options

Ce compte est administrateur global
Les administrateurs globaux ont les droits suivants :

- Accès complet à la configuration du serveur via WebAdmin
- Possibilité d'inclure tous les utilisateurs de tous les domaines dans ses contacts de messagerie instantanée
- Possibilité d'envoyer des messages aux listes même si l'accès est en "lecture seule".
- Possibilité d'envoyer des messages aux listes même s'il n'est pas membre.

Les administrateurs globaux ont un accès total à tous les fichiers et options de MDaemon. Pour plus d'informations concernant les options d'administrateur dans WebAdmin, voir la section concernant WebAdmin.

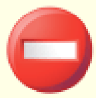
Ce compte est administrateur de domaine
Activez cette option pour accorder à l'utilisateur le droit Administrateur de domaine. Les administrateurs de domaine ont les mêmes droits que les administrateurs globaux mais ils sont limités au domaine auquel ils appartiennent. Pour en savoir plus sur les administrateurs de domaine, voir la section concernant WebAdmin.

Ce compte est privé
MDaemon crée et tient à jour automatiquement une liste de diffusion nommée "everyone@" pour chaque domaine, permettant d'envoyer un message à tous les

utilisateurs du domaine simultanément. Par défaut, MDaemon inclut tous les comptes dans cette liste. Activez cette option si vous souhaitez masquer le compte dans cette liste. Il sera également masqué dans les calendrier et les résultats VRFY .

Autoriser la modification des paramètres du compte par e-mail
Ce paramètre indique si l'utilisateur peut modifier ses paramètres de compte (par exemple son mot de passe, ses répertoires de messages) à distance, par e-mail, autrement dit en envoyant des messages spécialement formatés au serveur. Vous trouverez des explications complètes sur la manipulation de compte à distance dans : Contrôle du serveur à distance par e-mail 452.

Autoriser la modification du carnet d'adresses public
Sélectionnez cette option si vous souhaitez que le compte puisse ajouter et supprimer des entrées dans les carnets d'adresses publics WorldClient ou LDAP.



Si le compte synchronise des dossiers avec ComAgent, il est possible que les modifications s'étendent à tous les utilisateurs. Soyez attentif lorsque vous activez cette fonctionnalité.

Accepter automatiquement les requêtes de rendez-vous et traiter les annulations
Cette option traite automatiquement les requêtes, modifications et annulations de rendez-vous reçues par le compte. Lorsqu'un message concernant ces requêtes est reçu, le calendrier de l'utilisateur est mis à jour automatiquement. Par défaut, cette option est désactivée pour tous les comptes.

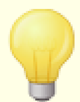
Utiliser les contacts en liste blanche et du carnet d'adresses par défaut en tant que liste blanche du Filtre anti-spam
La Liste blanche (automatique) 220 du Filtre anti-spam inclut une option qui permet d'annuler l'analyse anti-spam si l'expéditeur du message figure dans le carnet d'adresses par défaut ou la liste blanche personnelle de l'utilisateur. Décochez la case si vous avez activé cette option du Filtre anti-spam, mais que vous ne souhaitez pas l'appliquer à cet utilisateur.

Remarque : Avec ComAgent, vous pouvez facilement tenir à jour et synchroniser votre carnet d'adresses avec WorldClient, Outlook, Outlook Express ; le Carnet d'adresses Windows ou d'autres clients de messagerie qui utilisent le WAB.

Ajouter les destinataires des messages aux contacts en liste blanche
Lorsque cette option est activée, toutes les adresses auxquelles l'utilisateur envoie du courrier sont ajoutées à sa liste blanche personnelle. Associée à la précédente, cette option permet de réduire considérablement le nombre de faux positifs. Avant de l'activer, assurez-vous d'avoir également coché *Mettre à jour automatiquement les contacts en liste blanche* (dans l'onglet Liste blanche (automatique) 220 du Filtre anti-spam).

Remarque : cette option est désactivée pour les comptes qui utilisent l'autorépondeur.

Supprimer les contacts dont le nom ou le numéro de téléphone est manquant
Cliquez sur ce bouton si vous souhaitez supprimer tous les contacts contenant uniquement une adresse e-mail du carnet d'adresses par défaut de cet utilisateur. Si un contact n'a pas au moins un nom ou un numéro de téléphone il sera supprimé. Cette option est destinée à nettoyer les contacts ajoutés par l'option de liste blanche automatique des versions précédentes de MDaemon. En effet, dans les versions précédentes les adresses étaient ajoutées au carnet d'adresses par défaut au lieu de la liste blanche personnelle. Par conséquent les carnet d'adresses contenaient parfois des contacts que les utilisateurs ne souhaitaient pas ajouter.



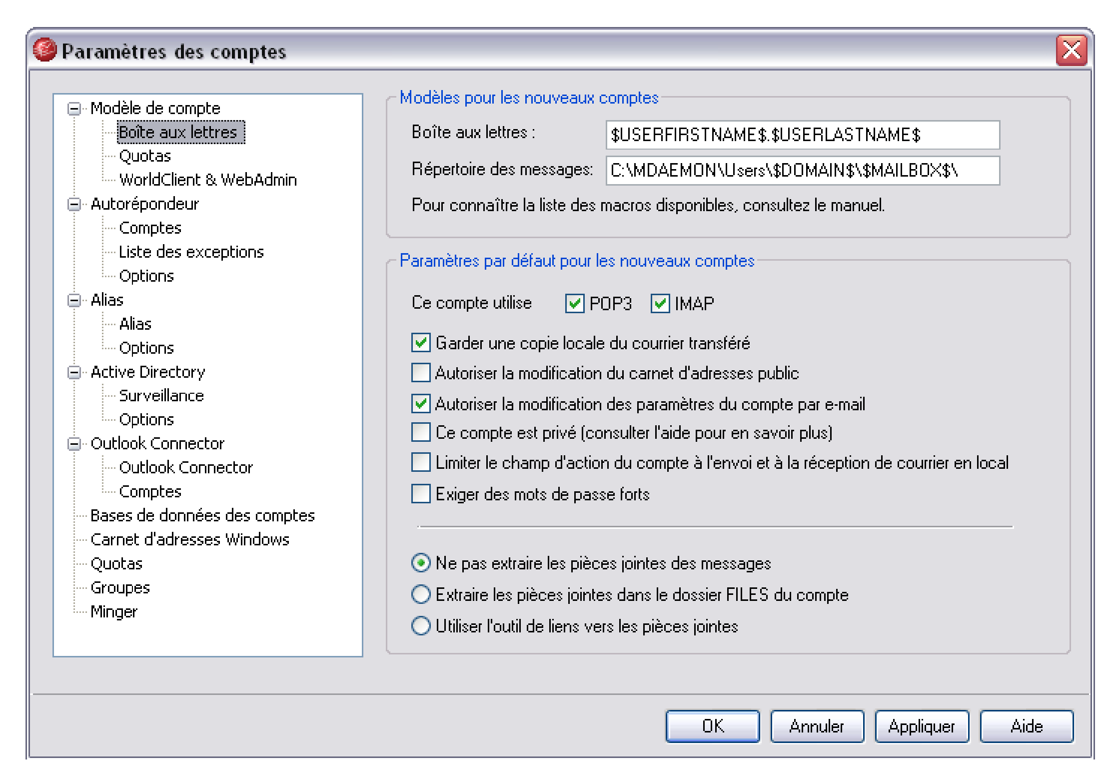
N'utilisez cette option qu'avec précaution, car des contacts contenant uniquement une adresse e-mail peuvent être légitimes.

Afficher toutes les listes de diffusion auxquelles ce compte appartient
Cliquez sur ce bouton pour afficher la liste des Listes de diffusion 378 dont ce compte est membre.

5.2 Paramètres des comptes

5.2.1 Modèle de compte

5.2.1.1 Boîte aux lettres



Cet onglet permet d'indiquer des valeurs par défaut pour divers paramètres de l'Éditeur de comptes301. De plus, il est possible d'utiliser des macros spécifiques333 dans les champs *Boîte aux lettres* et *Répertoire des messages* afin de générer automatiquement ces valeurs dès qu'un compte est créé ou importé.

Modèle pour les nouveaux comptes

Boîte aux lettres

Utilisez ce champ pour indiquer un modèle de nom de boîte aux lettres par défaut pour de nouveaux comptes. Cette valeur est également passée dans la commande USER POP qui permet d'accéder à une boîte aux lettres à distance ou depuis un client de messagerie POP. Voir Macros de modèles333 pour connaître la liste des macros pouvant être utilisées ici. Valeur par défaut : "$USERFIRSTNAME$.$USERLASTNAME$". Ainsi pour un utilisateur appelé Jean Dupond (dans le domaine exemple.com) le compte par défaut est jean.dupond@exemple.com.

Répertoire des messages

Utilisez ce champ pour indiquer un répertoire de messages par défaut pour les nouveaux comptes. Ces répertoires sont ceux dans lesquels les fichiers de messages distribués à une boîte aux lettres seront stockés. Assurez-vous qu'une fois étendu, le modèle fourni ici forme un chemin d'accès valide.



MDaemon contient un système de base pour la division des répertoires. Sous NTFS, par exemple, le fait de conserver plusieurs répertoires sous la même racine peut poser des problèmes. Pour les éviter, vous pouvez utiliser la macro $MAILBOXFIRSTCHARSn$, dans laquelle "n" représente un nombre entre 1 et 10. Cette macro s'étendra aux "n" premiers caractères du nom de la boîte aux lettres. En remplaçant le modèle de votre répertoire de messages par défaut, par un autre semblable à celui ci-dessous, vous obtiendrez un système de division de répertoire correct :

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\.
```

Paramètres par défaut pour les nouveaux comptes

Valeurs figurant par défaut dans l'Éditeur de compte pour les nouveaux comptes. Pour plus d'informations concernant ces options, voir Éditeur de compte301.

Ce compte utilise...

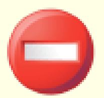
POP3

Par défaut, les comptes peuvent accéder à leur messagerie via des clients POP3. Décochez cette option si vous ne souhaitez pas accorder cet accès par défaut aux nouveaux comptes (défini dans l'onglet Informations du compte301 de l'Éditeur de compte).

IMAP
Par défaut, les comptes peuvent accéder à leur messagerie via des clients IMAP. Décochez cette option si vous ne souhaitez pas accorder cet accès par défaut aux nouveaux comptes (défini dans l'onglet Informations du compte 301 de l'Éditeur de compte).

Garder une copie locale du courrier transféré
Par défaut une copie de chaque message transféré est envoyée au compte (défini dans l'onglet Transfert 313 de l'Éditeur de compte).

Autoriser la modification du carnet d'adresses public
Sélectionnez cette option si vous souhaitez que par défaut, les nouveaux comptes puissent ajouter et supprimer des entrées dans les carnets d'adresses publics WorldClient ou LDAP (défini dans l'onglet Options 328 de l'Éditeur de compte).



Si le compte synchronise des dossiers avec ComAgent, il est possible que les modifications s'étendent à tous les utilisateurs. Soyez attentif lorsque vous activez cette fonctionnalité.

Autoriser la modification des paramètres du compte par e-mail
Activez cette option si vous souhaitez que par défaut, les nouveaux utilisateurs puissent modifier les paramètres de son compte en envoyant des e-mails spécialement formatés 452. Cette option détermine la valeur par défaut de l'option correspondante dans l'onglet Options 328 de l'Éditeur de compte.

Ce compte est privé
MDaemon crée et tient à jour automatiquement une liste de diffusion nommée "everyone@" pour chaque domaine, permettant d'envoyer un message à tous les utilisateurs du domaine simultanément. Par défaut, MDaemon inclut tous les comptes dans cette liste. Activez cette option si vous souhaitez masquer les nouveaux comptes dans cette liste. Il seront également masqués dans les calendrier et les résultats VRFY. Cette option détermine la valeur par défaut de l'option correspondante dans l'onglet Options 328 de l'Éditeur de compte.

Limiter le champ d'action du compte à l'envoi et à la réception de courrier en local
Cette option détermine les valeurs par défaut de l'onglet Restrictions 314 pour les nouveaux comptes. Si elle est activée, les nouveaux comptes peuvent uniquement envoyer ou recevoir du courrier sur le domaine local.

Gestion des pièces jointes
Cette option détermine la valeur par défaut de l'option correspondante dans l'onglet Courrier et pièces jointes 303 de l'Éditeur de comptes.

Ne pas extraire les pièces jointes des messages
Si cette option est sélectionnée, les pièces jointes ne sont pas extraites et les messages sont distribués normalement.

Extraire les pièces jointes dans le dossier FILES du compte
Si ce paramètre est activé, MDaemon extrait automatiquement les pièces jointes des messages entrants. Les fichiers extraits sont retirés des messages entrants et placés dans le répertoire \Files\ du compte (par défaut : C:\MDaemon\Users\<domaine>\<utilisateur>). Le corps du message indique les noms des fichiers extraits mais aucun lien n'est fourni pour les récupérer. L'utilisateur doit donc disposer d'un accès au dossier \Files\ de son compte.

Utiliser l'outil de liens vers les pièces jointes
Cette option extrait les pièces jointes des messages et les stocke à l'emplacement désigné dans la fenêtre Liens vers les pièces jointes139. Le corps du message contient des liens permettant à l'utilisateur de récupérer les pièces jointes extraites. Pour des raisons de sécurité, ces URL ne contiennent pas de chemins complet, mais un identifiant unique (GUID) que le serveur utilise pour lier le fichier. Les liaisons GUID sont définies dans le fichier `AttachmentLinking.dat`.



Si cette option est sélectionné, mais que le système n'est pas activé dans la fenêtre Liens vers les pièces jointes139, les pièces jointes ne seront pas extraites.

Exiger des mots de passe forts
Par défaut, MDaemon exige que les nouveaux comptes utilisent des mots de passe forts.

Les mots de passe forts :

- Contiennent un nombre minimum de caractères (par défaut : 6).
- Contiennent à la fois des lettres et de chiffres.
- Contiennent des majuscules ET des minuscules.
- Ne contiennent pas le nom de la boîte aux lettres ou le nom de l'utilisateur.

Vous pouvez modifier le nombre minimum de caractères requis en modifiant le fichier `MDaemon.ini` comme suit :

```
[Special]
MinPasswordLength=XX (par défaut : 6)
```

Voir également :

Macros de modèles 333
Éditeur de compte 301
Courrier et pièces jointes 303
Liens vers les pièces jointes 139

5.2.1.1.1 Macros de modèles

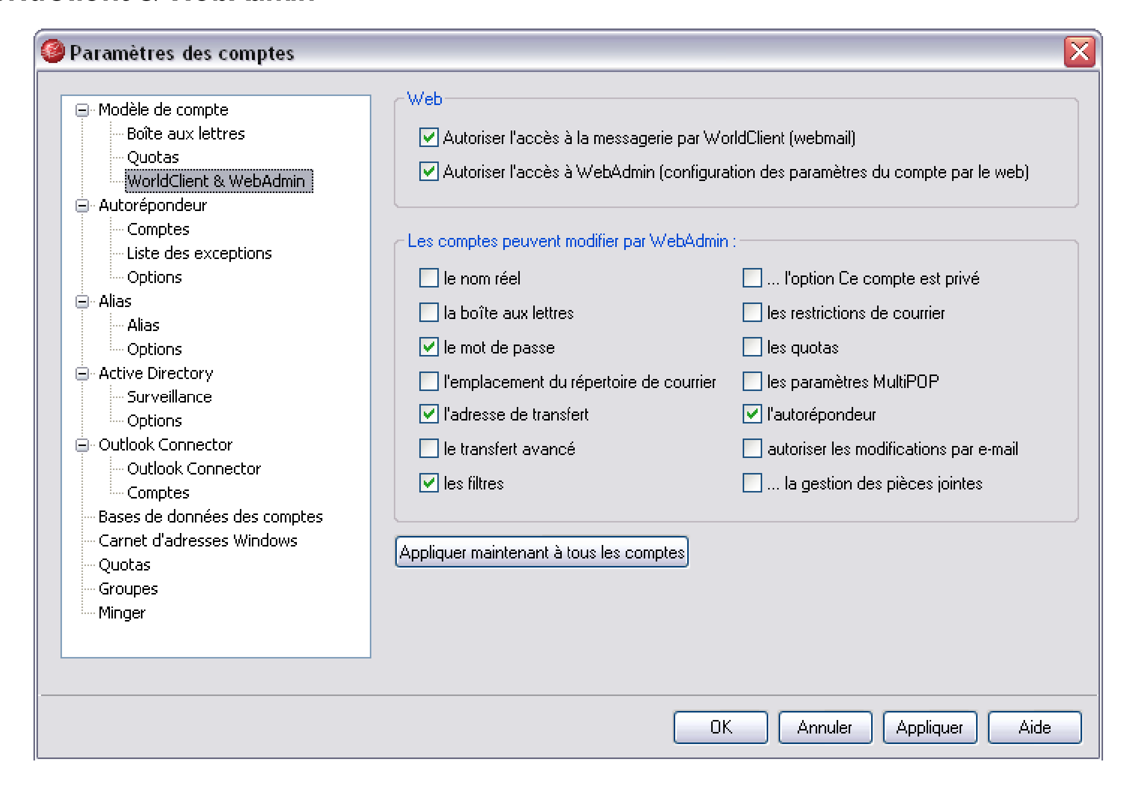
Voici les macros disponibles pour automatiser la configuration des nouveaux comptes.

$DOMAIN$	Résout le nom de domaine sélectionné pour le compte.
$DOMAINIP$	Résout l'IP associée au domaine actuellement sélectionné pour le compte.
$MACHINENAME$	Renvoie le nom de machine figurant dans l'onglet Domaine des propriétés du domaine par défaut. Cette macro est utilisée dans le script contenant les informations par défaut des nouveaux comptes (NEWUSERHELP.DAT).
$USERNAME$	Résout le prénom et le nom complet du détenteur du compte. Ce champ est équivalent à "$USERFIRSTNAME$$USERLASTNAME$".
$USERFIRSTNAME$	Résout le prénom du détenteur du compte.
$USERLASTNAME$	Cette variable résout le nom du détenteur du compte.
$USERFIRSTINITIAL$	Cette variable résout la première lettre du prénom du détenteur du compte.
$USERLASTINITIAL$	Cette variable résout la première lettre du nom du détenteur du compte.
$MAILBOX$	Cette variable résout le nom de boîte aux lettres du compte actuel. Cette valeur sera également utilisée comme nom d'utilisateur POP dans les sessions de messagerie POP3. Il s'agit de la valeur exigée dans la commande USER lors de la connexion de session POP.
$MAILBOXFIRSTCHARSn$	Remplacez "n" par un chiffre compris entre 1 et 10. Résout les "n" premiers caractères du nom de la boîte aux lettres.

Voir également :

Modèle de compte » Boîte aux lettres 330

5.2.1.2 WorldClient & WebAdmin



Cet onglet sert à indiquer les droits d'accès par défaut que les nouveaux comptes auront sur WorldClient 106 et WebAdmin 129. Vous pouvez indiquer si les comptes pourront ou non accéder à leur courrier via WorldClient et si les utilisateurs pourront ou non configurer leurs comptes via WebAdmin. De plus, si vous accordez l'accès à WebAdmin, vous pouvez contrôler les paramètres que les comptes pourront modifier.

Web

Autoriser l'accès à la messagerie par WorldClient

Activez cette option si vous voulez que les nouveaux comptes aient accès au serveur WorldClient 106 qui leur permet de vérifier leur courrier depuis un navigateur web.

Autoriser l'accès à WebAdmin (configuration des paramètres du compte par le web)

Activez cette fonctionnalité si vous voulez accorder des permissions aux utilisateurs de MDaemon pour modifier leurs paramètres de compte dans WebAdmin 129. Ils ne pourront modifier que les paramètres que vous avez indiqués dans cette boîte de dialogue.

Les comptes peuvent modifier par WebAdmin :

le nom réel

En activant cette fonctionnalité, les nouveaux utilisateurs pourront modifier le *Prénom et nom*.

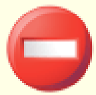
la boîte aux lettres
Autorise les nouveaux utilisateurs à modifier le nom de leur boîte aux lettres.



Le nom de la boîte aux lettres équivaut à l’adresse e-mail. Par conséquent, si l’utilisateur la modifie, les messages envoyés à l’ancienne adresse risquent d'être rejetés ou supprimés.

le mot de passe
Activez cette option si vous souhaitez autoriser les nouveaux utilisateurs à modifier leur mot de passe.

l’emplacement du répertoire de courrier
Activez cette option si vous souhaitez autoriser les nouveaux utilisateurs à modifier leur Répertoire de messages 303.



Faites attention lorsque vous accordez cette autorisation aux utilisateurs. En donnant la possibilité aux utilisateurs de modifier leur répertoire de messages, il est possible que vous leur donniez accès à tous les répertoires sur votre système.

l’adresse de transfert
Lorsque cette fonctionnalité est activée, les nouveaux utilisateurs peuvent modifier les paramètres de transfert 313.

le transfert avancé
Lorsque cette fonctionnalité est activée, les nouveaux utilisateurs peuvent modifier leurs paramètres de transfert avancés.

les filtres
Utilisez cette option pour permettre aux nouveaux utilisateurs de créer et de gérer leurs propres filtres de courrier 307. Cette fonctionnalité n’est disponible que dans MDaemon PRO.

l'option Ce compte est privé
Cochez cette case pour autoriser les nouveaux utilisateurs à activer l'option Ce compte est privé se trouvant dans l'onglet Options 328 de l'Éditeur de compte.

les restrictions de courrier
Cochez cette case pour autoriser les nouveaux utilisateurs à modifier les options de l’onglet Restrictions 314.

les quotas
Activez cette option si vous souhaitez autoriser les nouveaux comptes à modifier leurs paramètres de quota 317.

les paramètres MultiPOP
Activez cette option si vous souhaitez que les nouveaux utilisateurs puissent ajouter

des entrées et activer/désactiver la collecte MultiPOP 320.

l'autorépondeur
Activez cette option si vous voulez que les utilisateurs puissent ajouter, modifier ou supprimer des autorépondeurs 310 pour leurs comptes.

les modifications par e-mail
Activez cette option si vous souhaitez que les nouveaux utilisateurs puissent modifier les paramètres de leur compte en envoyant des e-mails spécialement formatés 452.

la gestion des pièces jointes
Activez cette option si vous souhaitez que les nouveaux utilisateurs puissent modifier les options de gestion des pièces jointes se trouvant dans l'onglet Courrier et pièces jointes 303 de l'Éditeur de compte.

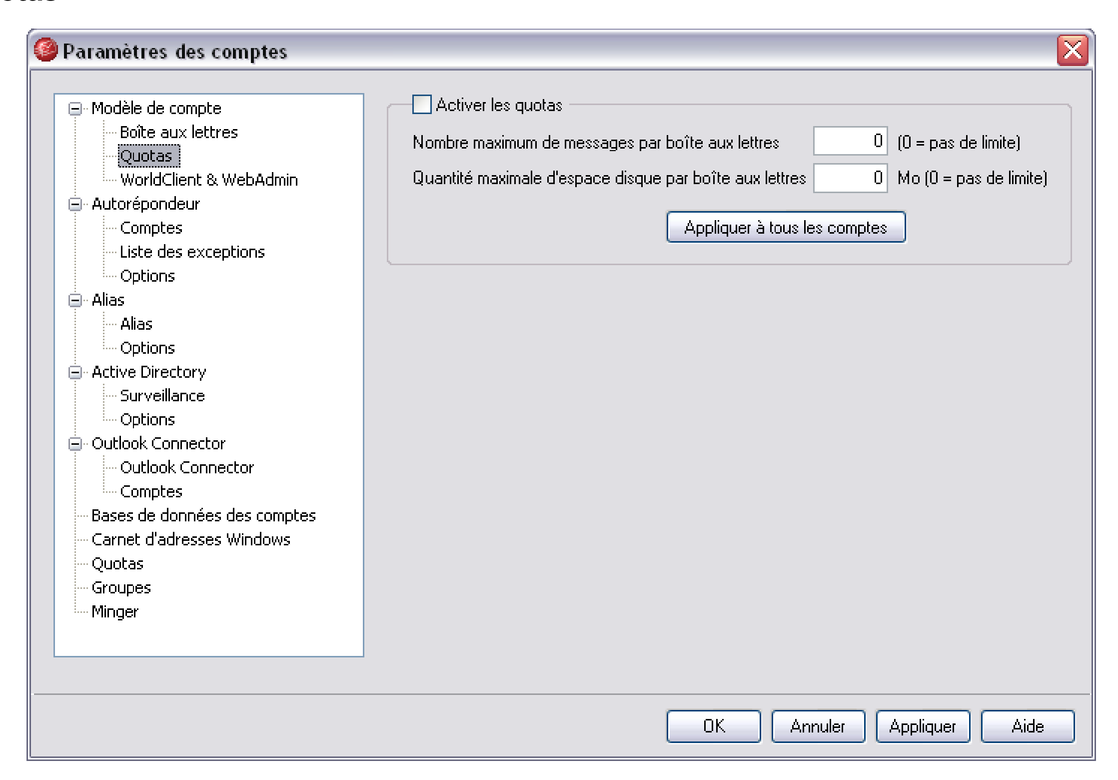
Appliquer maintenant à tous les comptes

Cliquez sur ce bouton pour que les paramètres par défaut s'appliquent à tous les comptes MDaemon. Attention : les autorisations d'accès Web existantes de tous les utilisateurs actuels de MDaemon seront remplacées par les valeurs indiquées ici. Il n'est pas possible d'annuler cette action.

Voir également :

Éditeur de compte » WorldClient & WebAdmin 304

5.2.1.3 Quotas



Cet onglet contient les valeurs par défaut figurant dans l'onglet Quotas317 pour les nouveaux comptes.

Quotas

Activer les quotas
Activez cette option si vous souhaitez appliquer des quotas aux nouveaux comptes. Si la réception d'un message entraîne le dépassement des quotas pour le nombre de messages ou l'espace disque, le message est refusé et un avertissement est placé dans le répertoire de courrier de l'utilisateur. Si une collecte MultiPOP dépasse la limite maximum du compte, un message d'avertissement similaire est émis et les entrées MultiPOP du compte sont automatiquement éteintes (mais ne sont pas retirées de la base de données).



Il est possible d'envoyer un message d'avertissement lorsqu'un certain pourcentage du quota est atteint, à l'aide de l'option située dans "Comptes » Paramètres des comptes » Quotas338". Ce message contient le nombre de messages et l'espace utilisés, les quantités autorisées, ainsi que l'espace restant. De plus, si un message d'avertissement se trouve déjà dans la boîte aux lettres, il est remplacé par le nouveau.

Nombre maximum de messages par boîte aux lettres
Indiquez ici le nombre maximal de messages pouvant être stockés pour chaque nouveau compte ("0" = pas de limite).

Quantité maximale d'espace disque par boîte aux lettres
Indiquez ici la quantité maximale d'espace disque pouvant être utilisé par chaque nouveau compte (y compris les pièces jointes enregistrées dans le dossier `\Files`). ("0" = pas de limite.)

Appliquer à tous les comptes

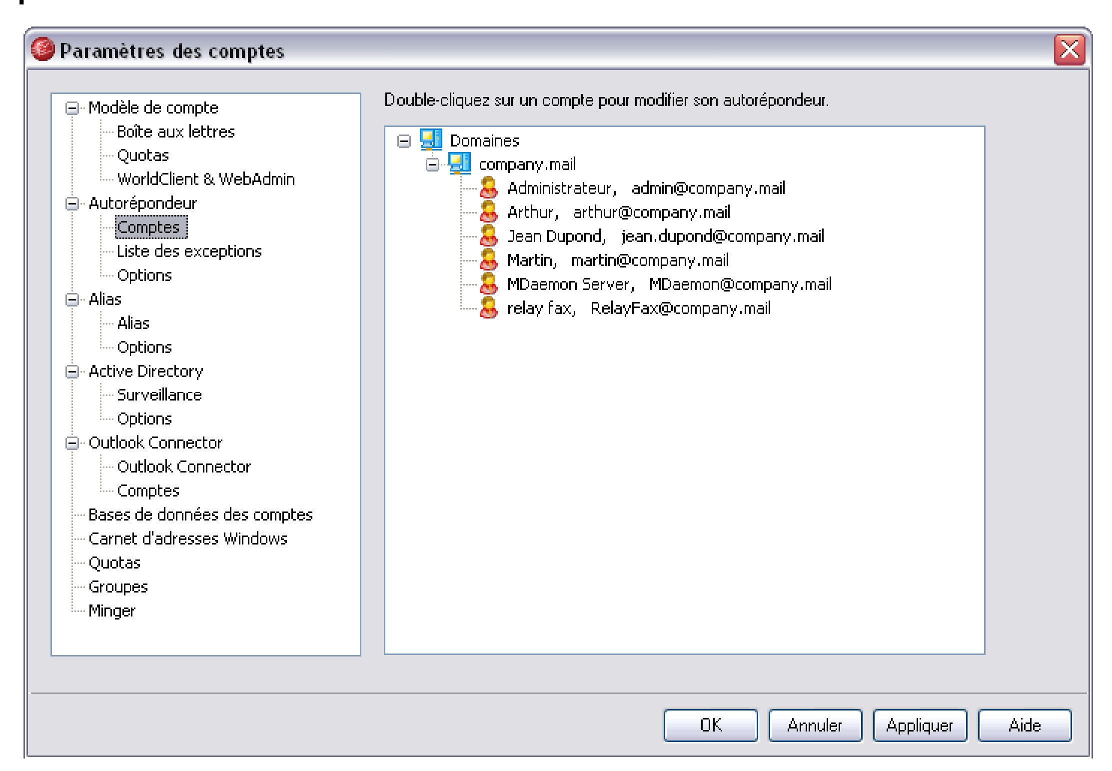
Cliquez sur ce bouton pour que les paramètres par défaut s'appliquent à tous les comptes MDaemon. Attention : les quotas existants de tous les utilisateurs actuels de MDaemon seront remplacés par les valeurs indiquées ici. Il n'est pas possible d'annuler cette action.

Voir également :

Éditeur de compte » Quotas 317
Paramètres des comptes » Quotas 367

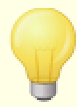
5.2.2 Autorépondeur

5.2.2.1 Comptes



Les autorépondeurs sont des outils permettant de déclencher des événements spécifiques lorsqu'un message entrant est reçu (exécuter un programme, ajouter l'expéditeur à une liste de diffusion, envoyer une réponse automatique...). Les autorépondeurs sont le plus couramment utilisés pour envoyer une réponse

automatique indiquant par exemple que le destinataire est absent, en congés, etc. Les utilisateurs disposant de droits d'accès web 304 à WorldClient 106 ou WebAdmin 129 disposent d'options leur permettant de choisir le contenu de la réponse automatique et définir les dates d'application de l'autorépondeur. Enfin, les messages de réponse automatique sont basés sur des fichiers de script (*.RSP) supportant un grand nombre de macros afin de personnaliser le message.



Les réponses automatiques sont toujours honorées lorsque le message déclencheur provient d'une source distante. Pour les messages locaux, le déclenchement de l'autorépondeur dépend de l'option *L'autorépondeur est déclenché par le courrier local*, située dans Autorépondeur » Options 342.

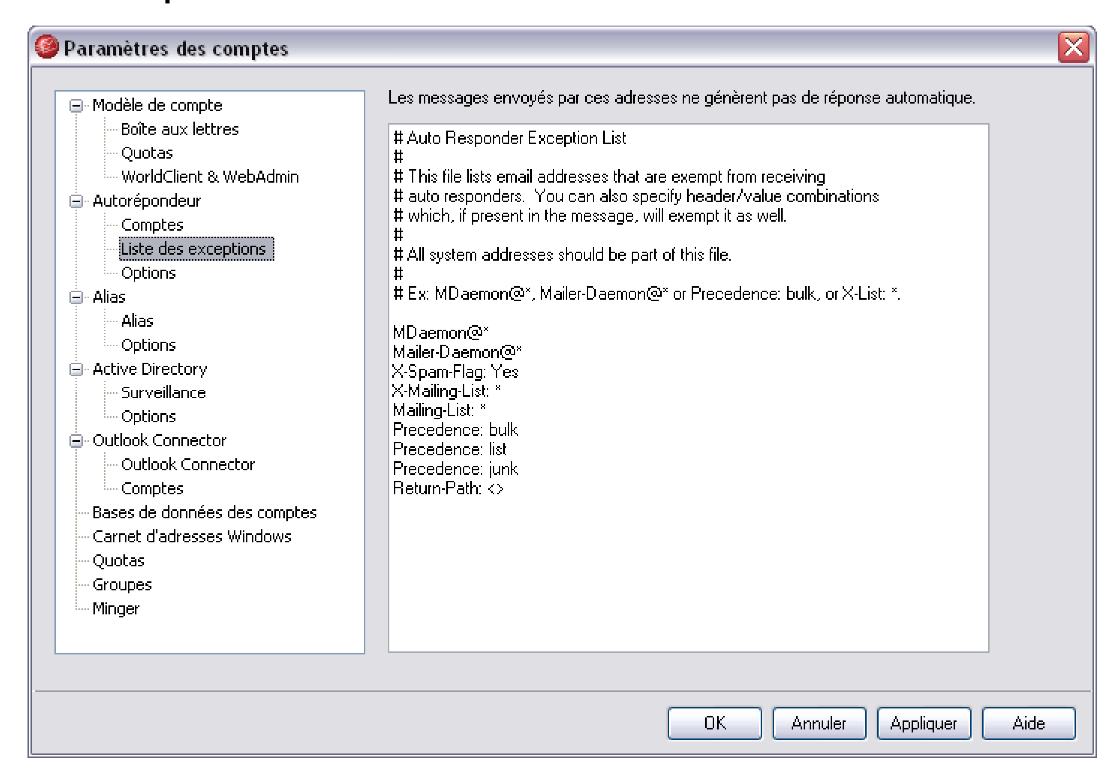
Liste des comptes

Cette liste affiche toutes les boîtes aux lettres locales pour lesquelles des autorépondeurs peuvent être configurés. Double-cliquez sur un compte de la liste pour ouvrir la boîte de dialogue Autorépondeur 310 et le configurer.

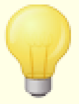
Voir également :

Autorépondeur » Liste des exceptions 341
Autorépondeur » Options 342
Création de scripts de réponse automatique 343
Éditeur de compte » Autorépondeur 310

5.2.2.2 Liste des exceptions



Les messages provenant d'adresses figurant dans cette liste ne reçoivent pas de réponse automatique. Vous pouvez indiquer des adresses e-mail ou bien des combinaisons en-tête/valeur. Une entrée par ligne. Les caractères jokers sont autorisés.

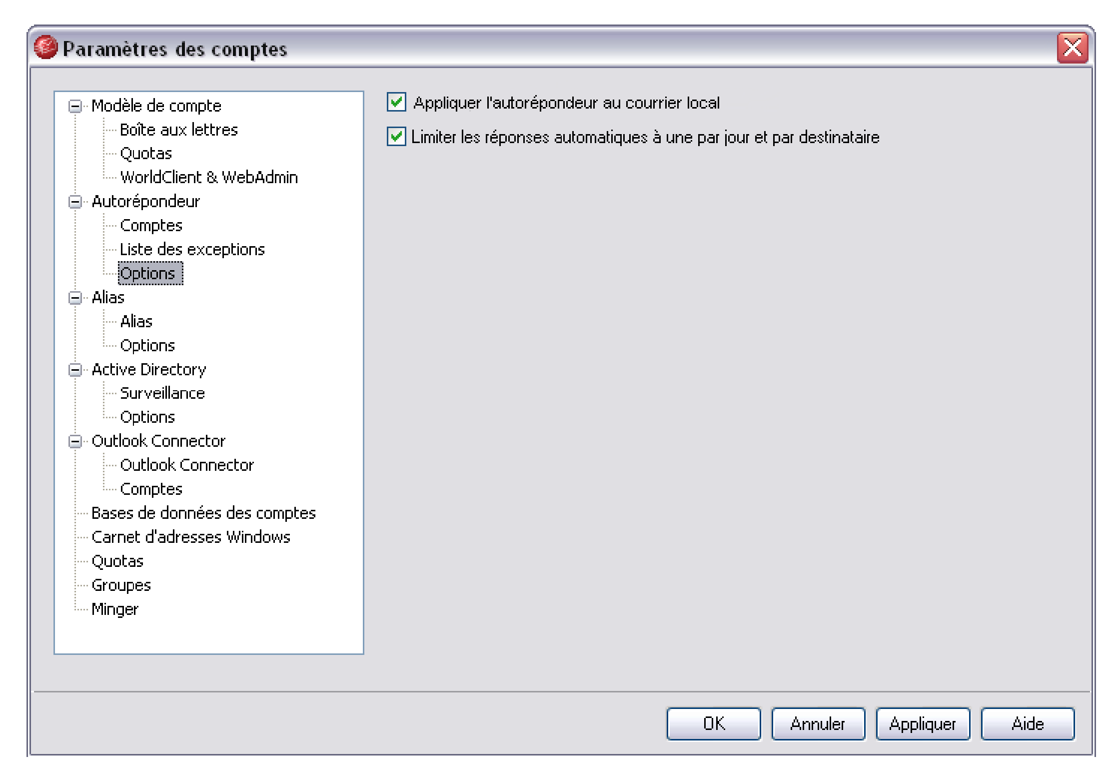


Toutes les adresses système (c'est-à-dire mdaemon@*, mailer-daemon@* , etc.) doivent être listées ici pour éviter les boucles de messagerie ou tout autre problème.

Voir également :

Autorépondeur » Comptes 339
Autorépondeur » Options 342
Création de scripts de réponse automatique 343
Éditeur de compte » Autorépondeur 310

5.2.2.3 Options



Options

Appliquer l'autorépondeur au courrier local
Décochez cette option si vous ne souhaitez pas que les autorépondeurs s'appliquent aux messages dont l'expéditeur ET le destinataire appartiennent à un domaine local.

Limiter les réponses automatiques à une par jour et par destinataire
Sélectionnez cette option pour limiter le nombre de réponses automatiques à une par jour et par destinataire. Cela évitera à une personne de recevoir plusieurs fois, dans la même journée, une réponse automatique identique à chaque fois qu'elle envoie du courrier.



Cette option évite également les boucles de courrier pouvant se produire lorsqu'une réponse automatique est envoyée à une adresse possédant elle-même un autorépondeur. Si elle n'est pas activée, des réponses automatiques risquent d'être envoyées indéfiniment d'une adresse à l'autre.

Voir également :

[Autorépondeur » Comptes](339)

[Autorépondeur » Options](342)

[Création de scripts de réponse automatique](343)

[Éditeur de compte » Autorépondeur](310)

5.2.2.4 Création de scripts de réponse automatique

Il s'agit de fichiers texte contenant les messages envoyés en tant que réponse automatique. Ce fichiers sont en texte clair ASCII et possèdent l'extension "`*.rsp`". Lorsqu'une réponse automatique est déclenchée, le contenu de ce fichier est analysé afin de remplacer les éventuelles macros par les données correspondantes. Les lignes commençant par "`#`" contiennent des commentaires et sont ignorées.

Vous trouvez ci-dessous divers exemples de scripts, et le répertoire `\app\` de MDaemon contient plusieurs fichiers "`*.rsp`" pouvant servir de modèles.

Macros pour les scripts de réponse automatique

`$HEADERS$`	Cette macro est remplacée par tous les en-têtes du message entrant ayant déclenché l'autorépondeur. Le texte indiqué juste avant cette macro est dupliqué au début de chaque ligne étendue.
`$HEADER:XX$`	Avec cette macro, la valeur de l'en-tête indiquée à la place de "xx" est étendue dans le message reformaté. Par exemple, s'il y a "TO: joe@mdaemon.com" dans le message d'origine, la macro $HEADER:TO$ s'étendra alors à "joe@mdaemon.com". S'il y a "Subject: Ceci est l'objet" dans le message d'origine, la macro $HEADER:SUBJECT$ sera alors remplacée par le texte "Ceci est l'objet".
`$BODY$`	Cette macro est remplacée par le corps du message dans sa totalité. Afin de préserver les jeux de caractères des différentes langues, MDaemon lit le corps du message comme des données binaires plutôt que comme du texte pur, afin de permettre une copie octet par octet du corps du message.
`$BODY-AS-TEXT$`	Comme la macro $BODY$, cette macro est remplacée par le corps du message dans sa totalité , sauf que MDaemon le lit comme un texte plutôt que comme des données binaires. Le texte indiqué juste avant cette macro est dupliqué au début de chaque ligne étendue. Ainsi, si vous utilisez "`>>$BODY-AS-TEXT$`" la réponse automatique affiche le corps du message et chaque ligne commence par "`>>`". Du texte peut également être ajouté à la droite de

cette macro.

$ATTACHMENTS$	Cette macro est remplacée par la liste complète de toutes les pièces jointes extraites dans le message d'origine. Le texte indiqué juste avant cette macro est dupliqué au début de chaque ligne étendue. Par exemple : `FILE-LIST: $ATTACHMENTS$` affiche le nom de chaque pièce jointe, précédé de "`FILE-LIST:`".
$ATTACHMENTCOUNT$	Cette macro est remplacée par un nombre entièr égal au nombre de pièces jointes extraites dans le message d'origine.
$ATTACHMENT(X)$	Cette macro est remplacée par le nom de fichier de la pièce jointe dont le "numéro" correspond à X. Si la valeur de X est supérieure au nombre total de fichiers attachés, la variable entière sera supprimée et ne sera pas remplacée.
$SENDER$	Cette macro résout l'adresse complète de l'expéditeur du message contenu dans l'en-tête "From:".
$SENDERMAILBOX$	Cette macro résout la boîte aux lettres de l'expéditeur du message. La boîte aux lettres est la portion de l'adresse électronique à gauche du symbole "@".
$SENDERDOMAIN$	Cette macro résout le domaine de l'expéditeur du message. Il s'agit de la portion de l'adresse électronique à droite du symbole "@".
$RECIPIENT$	Cette macro résout l'adresse complète du destinataire du message.
$RECIPIENTMAILBOX$	Cette macro résout la boîte aux lettres du destinataire du message. La boîte aux lettres est la portion de l'adresse électronique à gauche du symbole "@".
$RECIPIENTDOMAIN$	Cette macro résout le domaine du destinataire du message. Le domaine est la portion de l'adresse électronique à droite du "@".
$SUBJECT$	Cette macro résout la valeur de l'en-tête "Subject".
$MESSAGEID$	Cette macro résout la valeur de l'en-tête "Message-ID".

$CONTENTTYPE$	Cette macro résout la valeur de l'en-tête "Content-Type".
$PARTBOUNDARY$	Cette macro résout la valeur MIME "Part-Boundary" trouvée dans l'en-tête "Content-Type" des messages multipart.
$DATESTAMP$	Affiche la date et l'heure en respectant la RFC-2822.
$ACTUALTO$	Certains messages contiennent un champ "ActualTo" qui représente généralement la boîte aux lettres et l'hôte de destination dans la forme sous laquelle il a été saisi par l'utilisateur d'origine avant un reformatage ou une conversion d'alias.
$ACTUALFROM$	Certains messages contiennent un champ "ActualFrom" qui représente généralement la boîte aux lettres et l'hôte de l'expéditeur avant un reformatage ou une conversion d'alias.
$REPLYTO$	Cette macro résout la valeur trouvée dans l'en-tête "ReplyTo".
$PRODUCTID$	Numéro de version de version de MDaemon.

Macros de remplacement des en-têtes

Les macros ci-dessous remplacent le contenu des en-têtes des messages de réponse automatique.

%SetSender%
ex. : %SetSender%=mailbox@host.org
Cette macro remplace le contenu de l'en-tête TO. Par exemple, si l'expéditeur du message d'origine est "pooky@domain.com" et que l'autorépondeur utilise la macro %SetSender%="frank@example.com", l'en-tête TO de la réponse automatique contient "frank@example.com."

%SetRecipient%
ex: %SetRecipient%=mailbox@host.org
Cette macro remplace le contenu de l'en-tête FROM.

%SetReplyTo%
ex: %SetReplyTo%=mailbox@host.org
Cette macro remplace le contenu de l'en-tête ReplyTo.

%SetActualTo%
ex: %SetActualTo%=mailbox@host.org
Définit le destinataire "réel" du message.

%SetSubject%
ex: `%SetSubject%=Objet`
Remplace l'objet du message d'origine.

%SetMessageId%
ex: `%SetMessageId%=ID`
Remplace l'ID du message.

%SetPartBoundary%
ex: `%SetPartBoundary%=Boundary String`
Remplace la valeur part boundary.

%SetContentType%
ex: `%SetContentType%=MIME type`
Remplace la valeur content-type du message.

%SetAttachment%
ex: `%SetAttachment%=filespec`
Force MDaemon à joindre un fichier spécifique aux messages de réponse automatique.

5.2.2.4.1 Exemples de scripts de réponse automatique

Script simple utilisant diverses macros et appelé `VACATION.RSP` :

```
Cher  $SENDER$

Je suis dans l’impossibilité de lire votre message concernant
'$SUBJECT$' car je suis en
congés !
Cordialement,

$RECIPIENT$
```

Vous pouvez également utiliser les macros de remplacement des en-têtes :

```
Cher $SENDER$

Je suis dans l’impossibilité de lire votre message concernant
'$SUBJECT$' car je suis en
congés !
Cordialement,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\vacances.jpg
```

Avec ce script "`RE: `" est ajouté avant l'objet du message et une pièce jointe est aojutée.

La ligne "`%SetSubject%=RE: $SUBJECT$`" est traitée comme suit :

1. La portion `$SUBJECT$` est étendue et remplacée par l'objet du message d'origine. La chaîne est alors équivalente à :

   `%SetSubject%=RE: Original Subject Text`

2. MDaemon remplace l'objet d'origine qu'il a stocké dans sa mémoire interne par ce nouvel objet. A partir de ce moment, dès que "`$SUBJECT$`" est utilisé dans le script, le nouveau résultat est renvoyé.

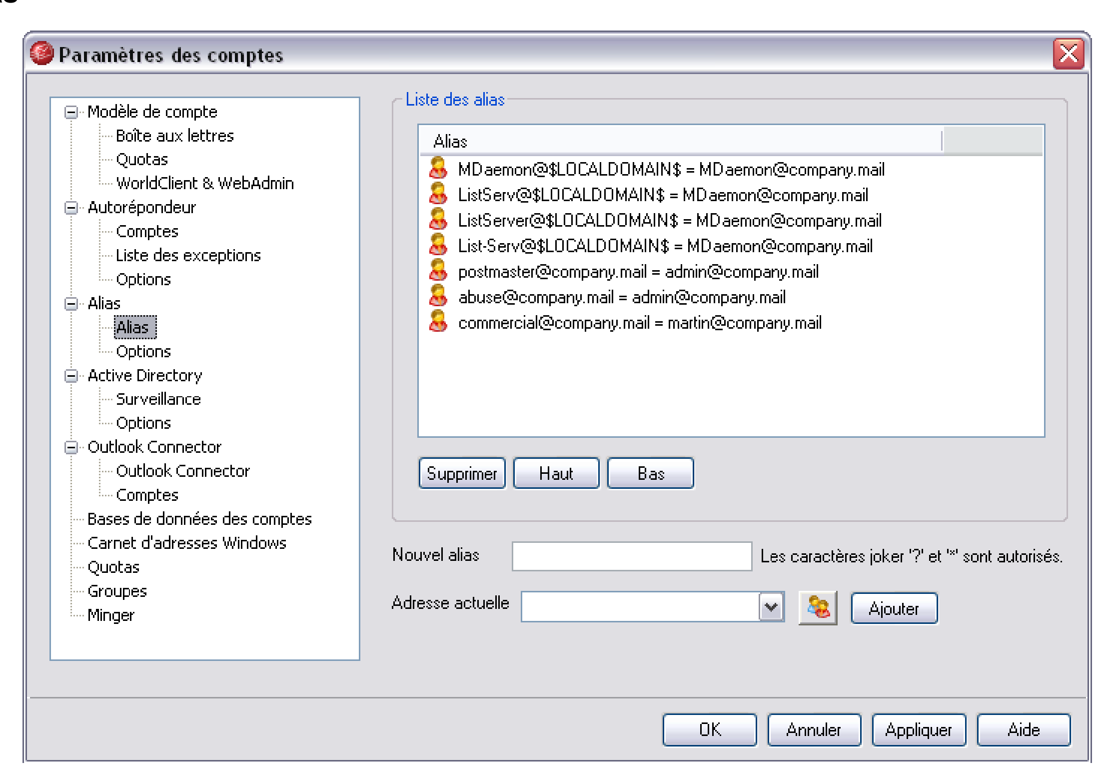
Les nouvelles macros se trouvent en bas du script de réponse, afin d'éviter des effets indésirables. Par exemple, si la macro %SetSubject% était placée avant la macro $SUBJECT$ qui se trouve dans la troisième ligne du script de réponse, le texte de l'objet aurait été modifié lors de l'expansion de la macro $SUBJECT$. Par conséquent, au lieu de remplacer $SUBJECT$ par le contenu de l'en-tête "Subject:" du message d'origine, elle sera remplacée par la valeur de votre choix que vous avez définie dans %SetSubject%.

Voir également :

Autorépondeur » Comptes 339
Autorépondeur » Liste blanche 341
Autorépondeur » Options 342
Éditeur de compte » Autorépondeur 310

5.2.3 Alias d'adresses

5.2.3.1 Alias



Les alias permettent de créer des noms de boîtes aux lettres supplémentaires pour vos comptes ou vos listes de diffusion, ce qui est particulièrement utile lorsque vous voulez que plusieurs noms de boîte aux lettres correspondent à un seul compte utilisateur ou une seule liste.

Par exemple, si Frank@altn.com traite toutes les demandes de renseignements concernant la facturation de votre domaine, mais que vous voulez que toutes les demandes soient adressées à Facturation@altn.com, vous pouvez créer un alias afin que les messages destinés à Facturation@altn.com soient en fait adressés à Frank@altn.com. Ou , si vous hébergez plusieurs domaines et que vous voulez que tous les messages destinés au postmaster (quel que soit le domaine) soient envoyés à `frank@example.com`, vous pouvez associer l'alias `Postmaster@*`, à cette adresse.

Liste des alias

Affiche tous les alias existants sur votre serveur.

Supprimer
Pour supprimer un alias de la liste, sélectionnez-le et cliquez sur ce bouton.

Haut
Les alias sont traités dans l'ordre de la liste. Vous pouvez déplacer un alias vers le haut de la liste en le sélectionnant, puis en cliquant sur ce bouton.

Bas
Vous pouvez déplacer un alias vers le bas de la liste en le sélectionnant, puis en cliquant sur ce bouton.

—

Nouvel alias
Entrez l'adresse électronique pour laquelle vous souhaitez créer un alias. Les jokers "?" et "*" sont autorisés, et vous pouvez utiliser la macro "@$LOCALDOMAIN$" pour remplacer uniquement vos domaines locaux. Par exemple : "marc@exemple.*", "*@$LOCALDOMAIN$" ou "marc@$LOCALDOMAIN$".

Adresse actuelle
Sélectionnez un compte dans la liste ou saisissez une adresse ou liste de diffusion dans ce champ, ou bien cliquez sur l'icône pour la sélectionner. Il s'agit de l'adresse réelle qui recevra le message lorsqu'il est adressé à un alias correspondant.

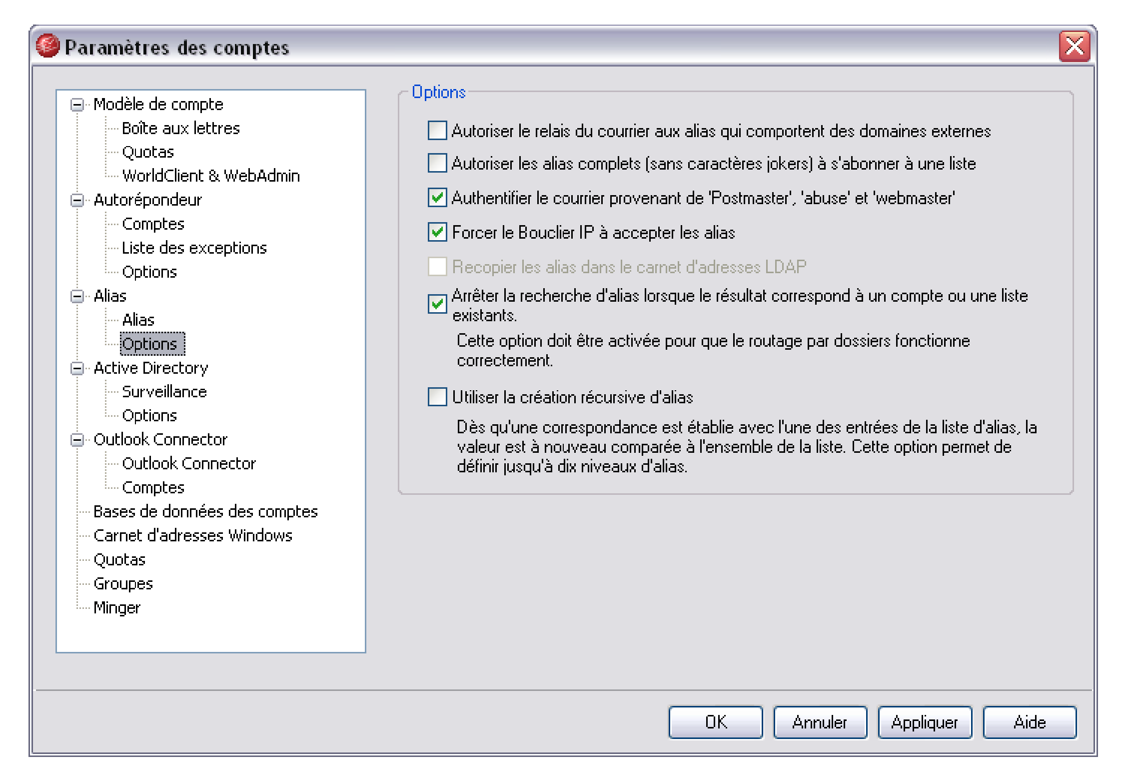
Ajouter
Après avoir rempli les deux champs ci-dessus, cliquez sur ce bouton pour ajouter un alias à la liste.

Voir également :

Alias » Options 349

Éditeur de compte » Alias 319

5.2.3.2 Options



Options

Autoriser le relais du courrier aux alias qui comportent des domaines externes
Cochez cette case si vous voulez que MDaemon relaie le courrier destiné à des alias contenant des domaines non locaux. Cette option annule les paramètre de Contrôle du relais 238 pour ces alias.

Autoriser les alias complets (sans caractères jokers) à s'abonner à une liste
Activez cette option pour que les alias soient autorisés à devenir membres des listes de diffusion de MDaemon. Si elle est désactivée, seuls les comptes réels peuvent devenir membres d'une liste. Remarque : les alias qui contiennent des caractères joker ne sont pas autorisés à s'abonner aux listes de diffusion, même si cette option est activée.

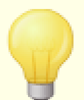
Authentifier le courrier provenant de 'Postmaster', 'abuse' et 'webmaster'
Lorsqu'un message prétend provenir des comptes postmaster, abuse, ou webmaster de vos domaines locaux, une authentification est exigée par défaut. En effet, les spammeurs savent que ces comptes existent sur tous les serveurs et essaient de les utiliser pour envoyer du spam. Cette option est également disponible Authentification SMTP 247 (Sécurité » Paramètres de sécurité). Lorsque cette option est modifiée dans l'un de ces emplacements, elle l'est également dans l'autre.

Forcer le Bouclier IP à accepter les alias
Par défaut, le Bouclier IP 240 accepte les alias d'adresses lors de la vérification de la correspondance domaine/IP. Il leur donne le nom de compte réel vers lequel ils pointent, et les accepte s'ils réussissent la vérification. Si cette option est

désactivée, le Bouclier IP traite chaque alias comme s'il était une adresse indépendante du compte qu'elle représente. Ainsi, si l'alias d'une adresse IP ne parvient pas à passer le bouclier IP, le courrier est refusé. Cette option se trouve également dans le Bouclier IP.

Recopier les alias dans le carnet d'adresses LDAP
Activez cette option pour que les alias soient recopiés dans le carnet d'adresses LDAP. Cette copie est indispensable pour que la fonctionnalité de vérification à distance de LDAP soit fiable. En revanche, si vous n'utilisez pas la vérification à distance, il n'est pas nécessaire de recopier les alias dans le carnet d'adresses LDAP. Vous économiserez ainsi du temps de traitement. Pour plus d'informations, voir LDAP 90.

Arrêter la recherche d'alias lorsque le résultat correspond à un compte ou une liste existants
Lorsque cette option est activée, la vérification des alias s'arrête dès que le destinataire d'un message entrant correspond à un compte ou une liste de diffusion. Cela s'applique généralement aux alias contenant des caractères joker. Par exemple, si vous avez défini l'alias "`*@exemple.com=frank@exemple.com`," avec cette option l'alias s'appliquera uniquement aux adresses qui n'existent pas sur le serveur. Ainsi, s'il existe un comtpe "`Henri@exemple.com`," les messages adressés à Henry sont bien distribués à son adresse car l'alias ne s'applique pas.



Cette option doit être activée si vous utilisez le routage par dossiers 309, afin d'éviter d'éventuels problèmes avec le traitement de ces messages.

Utiliser la création récursive d'alias
Cochez cette case pour que les alias soient traités de façon récursive. Lorsqu'une correspondance est établie avec un alias, la valeur trouvée est comparée avec l'ensemble de la liste des alias – il est possible de diviser les alias jusqu'à 10 niveaux. Par exemple, vous pouvez définir des alias comme suit :

```
durge@exemple.com = frank@exemple.com
frank@exemple.com = x@x.com
x@x.com = dwimble@mon-exemple.net
```

Ceci est identique à l'alias :

```
durge@exemple.com = dwimble@mon-exemple.net
```

Cela signifie également que :

```
frank@exemple.com = dwimble@mon-exemple.net
```

Voir également :

Alias 347



5.2.4 Active Directory

MDaemon peut être configuré de façon à contrôler Active Directory et créer, modifier, supprimer ou désactiver des comptes lorsque les comptes correspondants sont changés dans Active Directory.

Création de comptes

Lorsque cette fonctionnalité est activée, MDaemon interroge Active Directory à intervalles réguliers et compare les résultats avec ceux de la requête précédente. Si un compte est ajouté dans Active Directory, MDaemon le détecte et crée un compte de messagerie associé, comprenant tous les paramètres présents dans AD (nom complet, identifiant, boîte aux lettres, description et activé/désactivé).

Par défaut, les comptes ainsi créés sont ajoutés au domaine principal. Toutefois, il est également possible de le créer dans le domaine contenu dans l'attribut "UserPrincipalName" de Active Directory. Si ce domaine n'existe pas dans MDaemon, un nouveau domaine supplémentaire est créé automatiquement.

Suppression des comtpes

Plusieurs options sont disponibles pour gérer les comptes supprimés dans Active Directory : ne rien faire (conserver le compte MDaemon correspondant), supprimer, désactiver, ou bloquer le compte MDaemon (le courrier est conservé sur le serveur mais l'utilisateur ne peut y accéder).

Mise à jour des comptes

Lorsque MDaemon détecte des modifications dans les comptes Active Directory, il les applique automatiquement aux comptes de messagerie correspondants.

Synchronisation de MDaemon et Active Directory

Le bouton *Synchroniser maintenant* permet d'ajouter automatiquement dans MDaemon tous les comptes présents dans AD. Si un compte correspondant existe déjà dans MDaemon, il sera lié à celui de AD. Ainsi, les modifications apportées dans AD s'appliqueront également aux comptes de messagerie.

Authentification dynamique

Les comptes créés par cette fonctionnalité utilisent par défaut l'authentification dynamique. L'authentification dynamique est une technique utilisée par MDaemon afin de vérifier un compte sans connaître son mot de passe. Dans ce cas, l'utilisateur indique son identifiant (et mot de passe) Windows et MDaemon les transmet à Windows pour l'authentification.

Pour que cet outil fonctionne, vous devez indiquer dans l'onglet Surveillance352 le nom de domaine Windows à utiliser lors de la vérification des comptes. (MDaemon essaie de détecter le nom de domaine afin que ce champ soit rempli automatiquement). Toutefois, il est possible de choisir un autre domaine, ou d'indiquer "NT_ANY" pour autoriser l'authentification sur tous vos domaines Windows. Si vous ne remplissez pas ce champ, MDaemon n'utilise pas l'authentification dynamique. Dans ce cas, MDaemon attribue un mot de passe de façon aléatoire, qui doit être modifié manuellement pour que les comptes puissent fonctionner.

Contrôle constant

Lorsque la vérification Active Directory est activée, elle fonctionne même si MDaemon est arrêté. Toutes les modifications apportées seront prises en compte dès le démarrage du serveur.

Sécurité

Toutes les opérations sont effectuées à sens unique, c'est à dire de Active Directory vers MDaemon. Par conséquent, cette fonctionnalité ne modifie en aucun cas les fichiers de Active Directory.

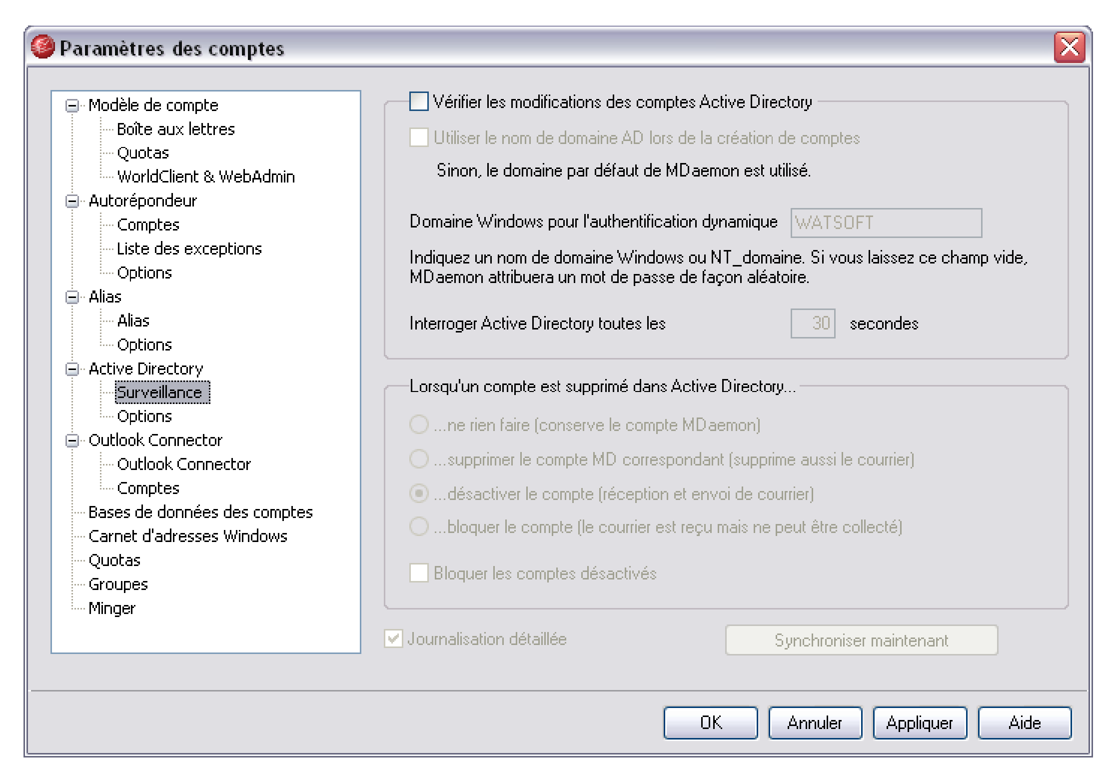
Modèle Active Directory

Lorsque MDaemon ajoute ou modifie des comptes suite à des modifications dans Active Directory, il utilise un modèle (/app/ActiveDS.dat) afin de lier certains attributs AD aux champs des comptes MDaemon. Par exemple, l'attribut « cn » est lié par défaut au champ "FullName". Ces liaisons ne sont pas cependant pas "codées en dur" : il suffit d'ouvrir le fichier ActiveDS.dat dans le Bloc-notes pour les modifier. Par exemple, vous pouvez remplacer "FullName=%cn%" par "FullName=%givenName% %sn%". Consultez le fichier `ActiveDS.dat` pour en savoir plus.

Voir également :

Active Directory » Surveillance 352
Active Directory » Options 354

5.2.4.1 Surveillance



Active Directory

Vérifier les modifications des comptes Active Directory
Cochez cette option pour activer le support Active Directory.

Utiliser le nom de domaine AD lors de la création de comptes
Cochez cette option si vous souhaitez que les comptes créés soient ajoutés au domaine figurant dans l'attribut Active Directory `UserPrincipalName`. Si ce domaine n'existe pas, un nouveau domaine supplémentaire est automatiquement ajouté à MDaemon. Lorsque cette option est décochée, tous les nouveaux comptes sont ajoutés au domaine par défaut de MDaemon.

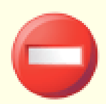
Domaine Windows pour l'authentification dynamique
Indiquez ici un nom de domaine Windows si vous souhaitez que les comptes créés utilisent l'authentification dynamique. Si vous ne remplissez pas ce champ, MDaemon n'utilise pas l'authentification dynamique. Dans ce cas, MDaemon attribue un mot de passe de façon aléatoire, qui doit être modifié manuellement pour que les comptes puissent fonctionner.

Interroger Active Directory toutes les XX secondes
Indiquez à quel intervalle MDaemon doit vérifier les comptes Active Directory.

Lorsqu'un compte est supprimé dans Active Directory :
Sélectionnez l'action à effectuer lorsque des comptes sont supprimés dans Active Directory.

...ne rien faire
Cochez cette option si vous souhaitez conserver le compte MDaemon lorsque le compte correspondant est supprimé dans Active Directory.

...supprimer le compte MD correspondant
Cochez cette option si vous souhaitez supprimer le compte MDaemon lorsqu'un compte est supprimé dans Active Directory.



Dans ce cas, tous les messages, dossiers, carnet d'adresses, calendriers, etc., du compte seront également supprimés.

...désactiver le compte
Le compte MDaemon est conservé sur le serveur, mais il ne peut pas envoyer ni recevoir de courrier et il n'est pas accessible pour les utilisateurs.

...bloquer le compte
MDaemon accepte le courrier destiné à ce compte, mais l'utilisateur ne peut pas y accéder : le courrier est "bloqué" sur le serveur.

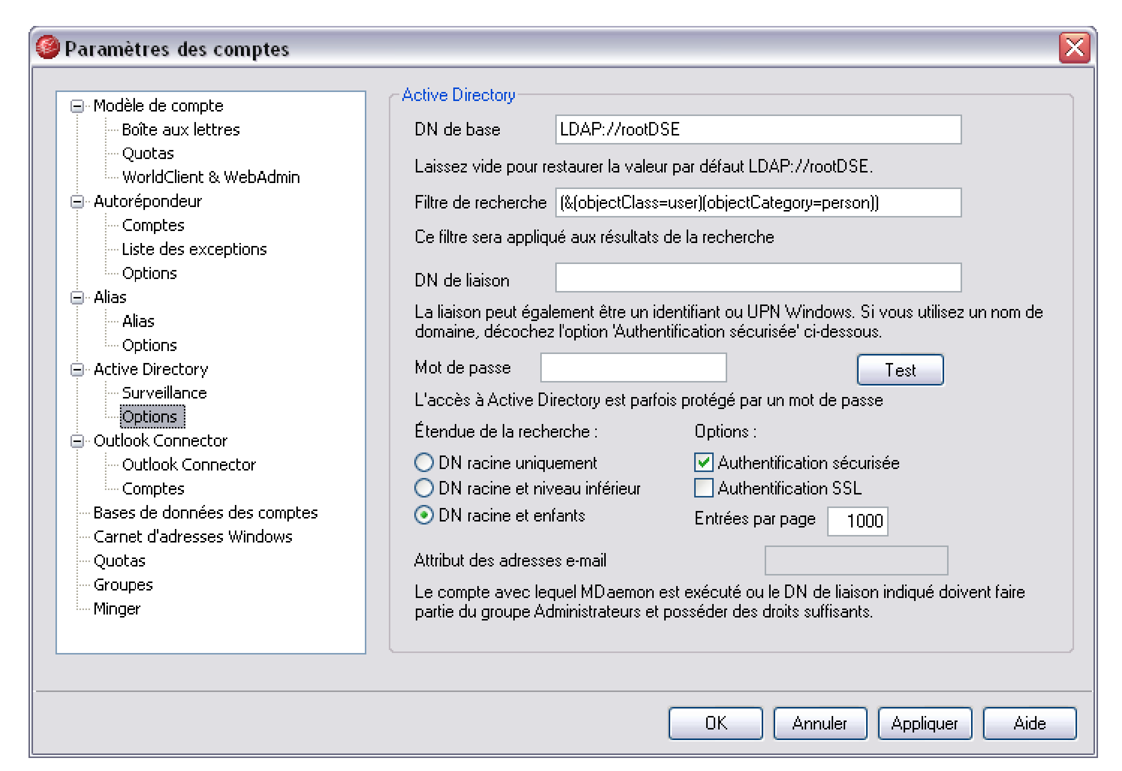
Bloquer les comptes désactivés
Par défaut, lorsqu'un compte est désactivé dans Active Directory, le compte MDaemon associé est également désactivé : MDaemon n'accepte pas les messages

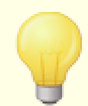
qui lui sont destinés et l'utilisateur ne peut pas y accéder. Cochez cette option si vous souhaitez que le compte MDaemon soit bloqué au lieu d'être désactivé.

Journalisation détaillée
Par défaut, MDaemon utilise une journalisation détaillée pour Active Directory. Désactivez cette option si vous souhaitez que les informations enregistrées soient moins complètes.

Synchroniser maintenant
Lorsque vous cliquez sur ce bouton, MDaemon interroge la base de données de Active Directory et crée, modifie ou supprime des comptes en fonction des paramètres choisis. Si un compte Active Directory correspond à un compte MDaemon existant, les deux comptes sont liés.

5.2.4.2 Options





L'accès à Active Directory requiert parfois des permissions spécifiques.

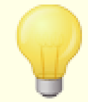
Options Active Directory

Nom de domaine
DN racine de l'arborescence, dans lequel MDaemon recherche les comptes. Par défaut, il recherche "Root DSE", qui correspond au point le plus haut dans la

hiérarchie de Active Directory. Vous pouvez réduire la durée de la recherche en désignant un point de départ plus près de l'emplacement des comptes dans votre arborescence. Si vous ne remplissez pas ce champ, MDaemon utilise la valeur par défaut : `LDAP://rootDSE`

Filtre de recherche
Filtre de recherche LDAP appliqué lors de la vérification des comptes dans Active Directory. Il permet de déterminer de façon plus précise les comptes que vous souhaitez inclure.

DN de liaison
DN utilisé par MDaemon pour effectuer la liaison avec Active Directory. Vous pouvez indiquer un compte Windows ou un chemin UPN.



Si vous utilisez un DN au lieu d'un identifiant Windows, vous devez désactiver l'option *Authentification sécurisée* ci-dessous.

Mot de passe
Mot de passe correspondant au DN ou à l'identifiant Windows défini dans l'option précédente.

Test
Cliquez sur ce bouton pour tester la configuration des paramètres Active Directory de MDaemon.

Étendue de la recherche :

DN racine uniquement
Limite la recherche au DN indiqué ci-dessus.

DN racine et niveau inférieur
Étend la recherche au niveau situé au-dessous du DN racine dans l'arborescence.

DN racine et enfants
Étend la recherche à tous les enfants du DN racine, jusqu'au niveau le plus bas. Cette option est appliquée par défaut.

Options :

Authentification sécurisée
Cochez cette option si vous souhaitez utiliser une authentification sécurisée lors des recherches dans Active Directory. Vous ne pouvez pas l'utiliser si vous avez choisi un DN et non un identifiant Windows pour le champ *DN de liaison*.

Authentification SSL
Cochez cette option si vous souhaitez utiliser une authentification SSL lors des recherches dans Active Directory.



Cette option requiert un serveur et une infrastructure SSL dans votre réseau Windows et Active Directory. En cas de doute, contactez votre administrateur réseau.

Entrées par page
Si les résultats d'une requête Active Directory sont supérieurs au nombre d'entrées indiquées, ils seront inclus dans plusieurs pages. Indiquez ici le nombre maximum d'entrées par page.

Attribut des adresses e-mail

Cet attribut est utilisé pour les listes de diffusion MDaemon et n'est disponible que dans l'onglet Active Directory de l'éditeur de Listes de diffusion 395.

5.2.5 Outlook Connector for MDaemon

MDaemon PRO supporte Outlook Connector, un module additionnel vendu séparément disponible auprès de l'éditeur Alt-N Technologies. Outlook Connector permet de partager les calendriers, contacts, tâches etc. que vous possédez dans Microsoft Outlook avec d'autres utilisateurs – d'habitude, cela n'est possible que lorsque Outlook est couplé à Microsoft Exchange Server. Avec Outlook Connector vous disposez d'un environnement de travail collaboratif sans devoir posséder de serveur Exchange.

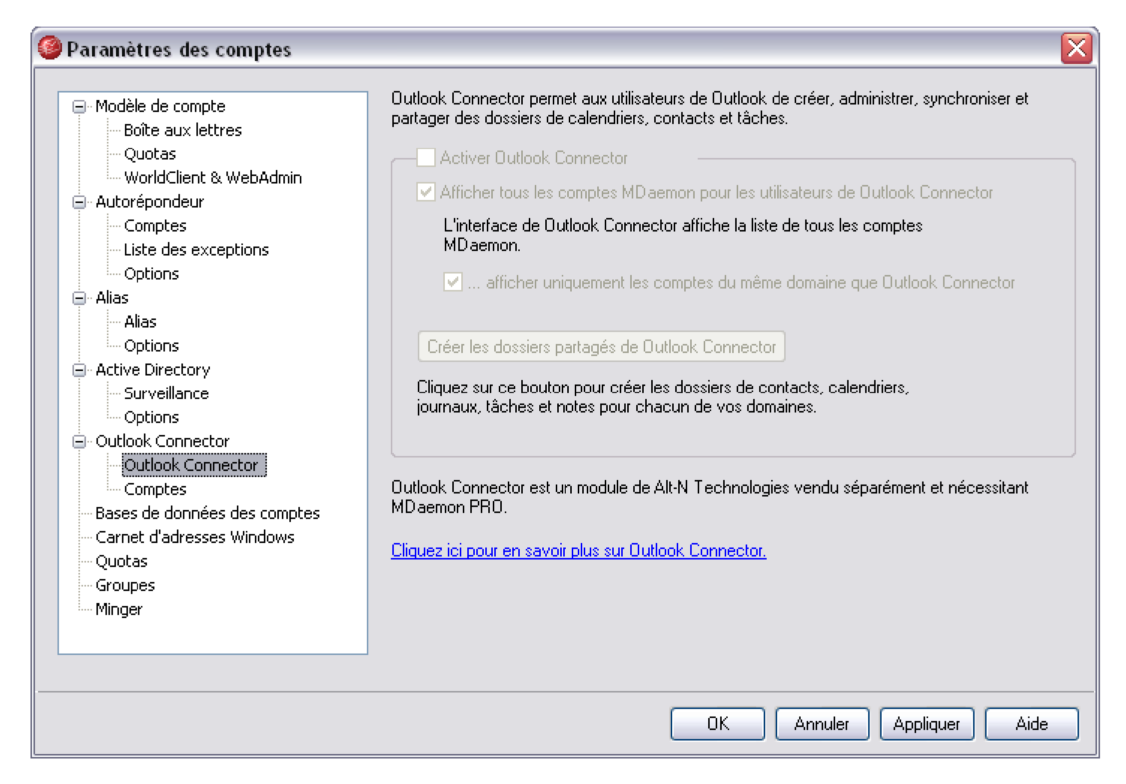
Une fois Outlook Connector for MDaemon installé, il s'active et se configure dans : Comptes » Paramètres des comptes » Outlook Connector.

Pour en savoir plus ou télécharger Outlook Connector, consultez les pages Outlook Connector for MDaemon sur le site www.altn.com.

Voir également :

Options Outlook Connector 357
Comptes Outlook Connector 358

5.2.5.1 Options Outlook Connector



Outlook Connector

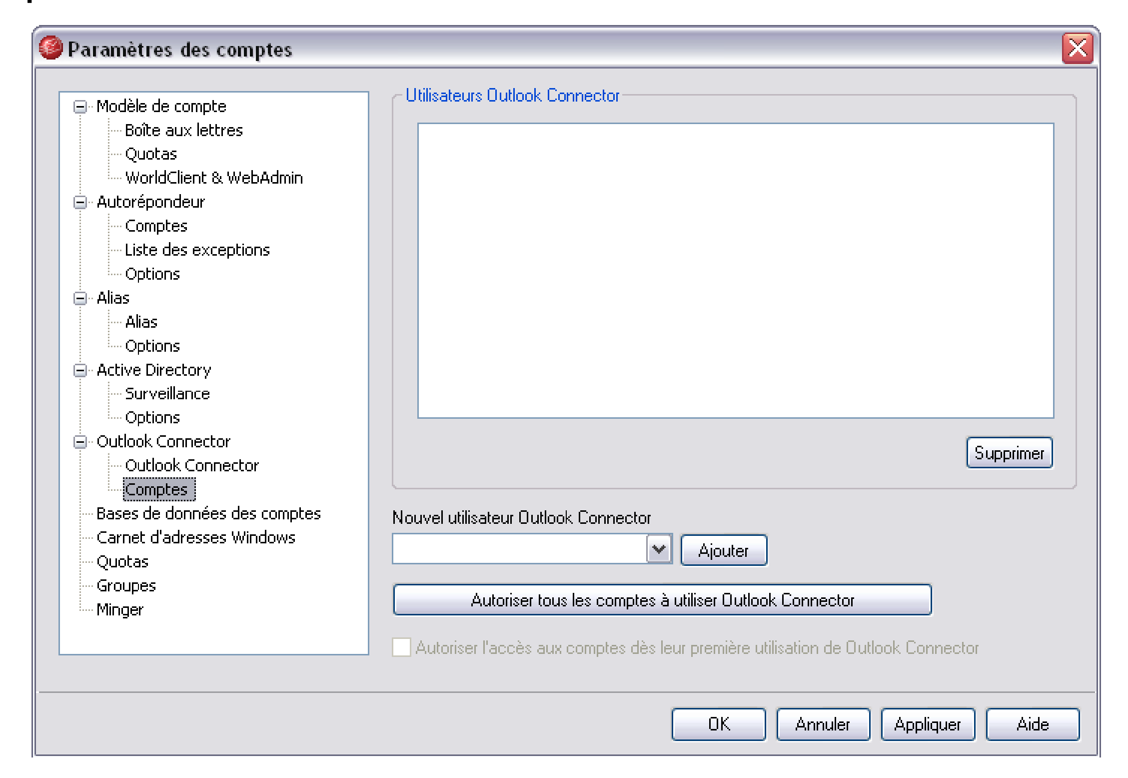
Activer Outlook Connector
Cette option active Outlook Connector. Vos utilisateurs ne peuvent pas bénéficier des fonctionnalités de Outlook Connector tant qu'elle n'est pas cochée.

Afficher tous les comptes MDaemon pour les utilisateurs de Outlook Connector
Sélectionnez cette option pour que tous les comptes MDaemon autorisés dans Outlook Connector soient visibles sur la liste des droits d'accès apparaissant dans le module Outlook Connector for MDaemon. Lorsqu'un utilisateur partage un élément dans Outlook, il choisit dans cette liste les comptes auxquels il souhaite accorder des droits. Lorsque cette fonctionnalité est désactivée, la liste de droits d'accès de Outlook Connector est vide et l'utilisateur doit saisir manuellement les adresses électroniques (seules les adresses appartenant à des comptes autorisés dans Outlook Connector pourront effectuer le partage). Si un utilisateur saisit une adresse qui n'est pas autorisée, les éléments ne seront pas partagés tant que l'adresse n'obtiendra pas d'autorisation.

...afficher uniquement les comptes du même domaine que Outlook Connector
Cette option n'est disponible que si l'option ci-dessus est activée. Cochez cette case si vous souhaitez que seuls les comptes autorisés dans Outlook Connector et appartenant au même domaine, apparaissent sur la liste de droits d'accès. Les comptes appartenant à des domaines différents ne seront pas répertoriés, même s'ils sont autorisés à utiliser Outlook Connector.

Créer les dossiers partagés de Outlook Connector
Cliquez sur ce bouton pour créer un ensemble de dossiers Outlook Connector pour chaque domaine : contacts, calendrier, journal, tâches et notes.

5.2.5.2 Comptes



Utilisateurs Outlook Connector

Il s'agit de la liste des utilisateurs MDaemon qui sont autorisés à partager leurs dossiers, calendriers, contacts, notes, etc. Outlook via Outlook Connector. Vous pouvez ajouter des utilisateurs à la liste en utilisant les options ci-dessous.

Nouvel utilisateur Outlook Connector
Pour ajouter un utilisateur MDaemon à la liste des utilisateurs autorisés, sélectionnez-le dans la liste déroulante puis cliquez sur *Ajouter*.

Ajouter
Après avoir sélectionné un utilisateur dans la liste déroulante *Nouvel utilisateur Outlook Connector*, cliquez sur ce bouton pour ajouter son compte à la liste.

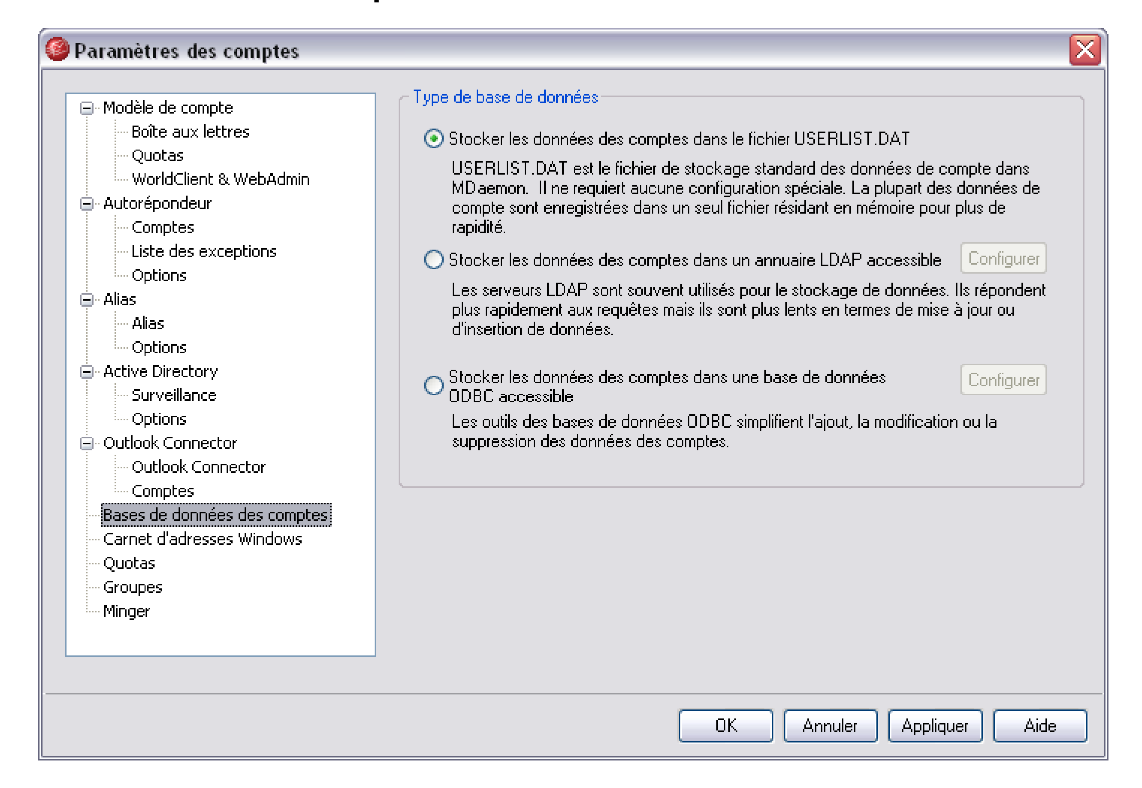
Supprimer
Pour supprimer un utilisateur de la liste, sélectionnez-le et cliquez sur ce bouton.

Autoriser tous les comptes à utiliser Outlook Connector
Cliquez sur ce bouton pour autoriser immédiatement tous les comptes MDaemon à

utiliser Outlook Connector. Tous les comptes MDaemon sont alors ajoutés à la liste des comptes autorisés.

Autoriser l'accès aux comptes dès leur première utilisation de Outlook Connector
Cochez cette case si vous souhaitez que les utilisateurs MDaemon soient ajoutés à la liste des comptes autorisés dès leur première utilisation de Outlook Connector. **Remarque :** cela revient à autoriser tous les comptes MDaemon à utiliser Outlook Connector for MDaemon. Ces comptes sont simplement ajoutés à la liste uniquement lorsqu'ils utilisent Outlook Connector pour la première fois.

5.2.6 Bases de données des comptes



Cette boîte de dialogue se trouve dans Comptes » Paramètres des comptes) et permet de désigner l'emplacement dans lequel sont stockés les comptes de MDaemon : le système local `USERLIST.DAT`, une base ODBC ou une base LDAP.

Stocker les données de comptes dans le fichier USERLIST.DAT
Sélectionnez cette option si vous voulez que MDaemon utilise son fichier interne USERLIST.DAT comme base de données de comptes. Il s'agit du paramètre par défaut de MDaemon. Avec cette option, toutes les informations de comptes utilisateurs MDaemon sont stockées localement. La plupart des informations sont stockées dans un fichier unique résidant en mémoire pour plus de rapidité et d'efficacité.

Stocker les données de comptes dans un annuaire LDAP accessible
Sélectionnez cette option si vous voulez que MDaemon utilise votre serveur LDAP

comme base de données de comptes utilisateurs plutôt que ODBC ou son système de fichier local USERLIST.DAT. Vous pouvez utiliser cette méthode pour maintenir les données de vos comptes utilisateurs si vous disposez de plusieurs serveurs MDaemon à des emplacements différents, mais souhaitez qu'ils partagent la même base de données d'utilisateurs. Chaque serveur MDaemon sera configuré pour se connecter au même serveur LDAP afin de partager les informations des utilisateurs plutôt que de les stocker localement. Les serveurs LDAP sont rapides en requêtes mais plus lents pour les mises à jour ou l'insertion de nouvelles données.

Configurer
Lorsque vous avez sélectionné l'option ci-dessus, cliquez sur ce bouton pour ouvrir la boîte de dialogue d'options LDAP 90 afin de configurer les paramètres de votre serveur LDAP.

Stocker les données de comptes dans une base de données ODBC accessible
Sélectionnez cette option si vous voulez utiliser une base de données compatible ODBC comme base de données de comptes MDaemon.

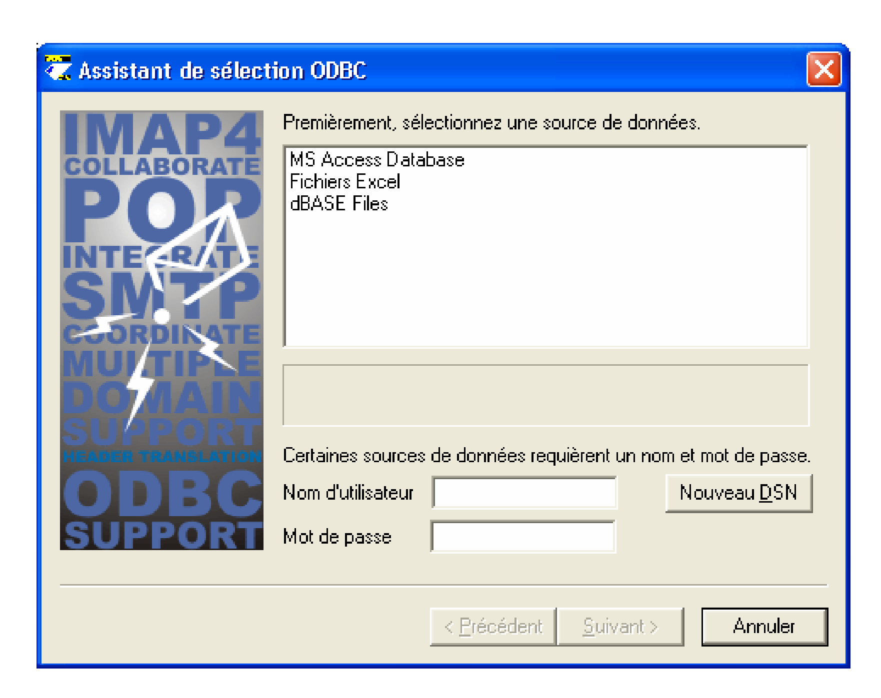
Configurer
Lorsque vous avez sélectionné l'option ci-dessus, cliquez sur ce bouton pour ouvrir l' assistant de sélection ODBC 360 afin de sélectionner et de configurer votre base de données compatible ODBC.

5.2.6.1 Assistant de sélection ODBC

Utilisez cet assistant pour sélectionner ou configurer une source de données système compatible ODBC à utiliser comme base de données de vos comptes MDaemon.

Migration de votre base de données de comptes vers un annuaire ODBC

1. Dans Comptes » Paramètres des comptes » Base de données des comptes, sélectionnez l'option *Stocker les données de comptes dans une base de données ODBC accessible* puis cliquez sur *Configurer* pour ouvrir l'assistant.

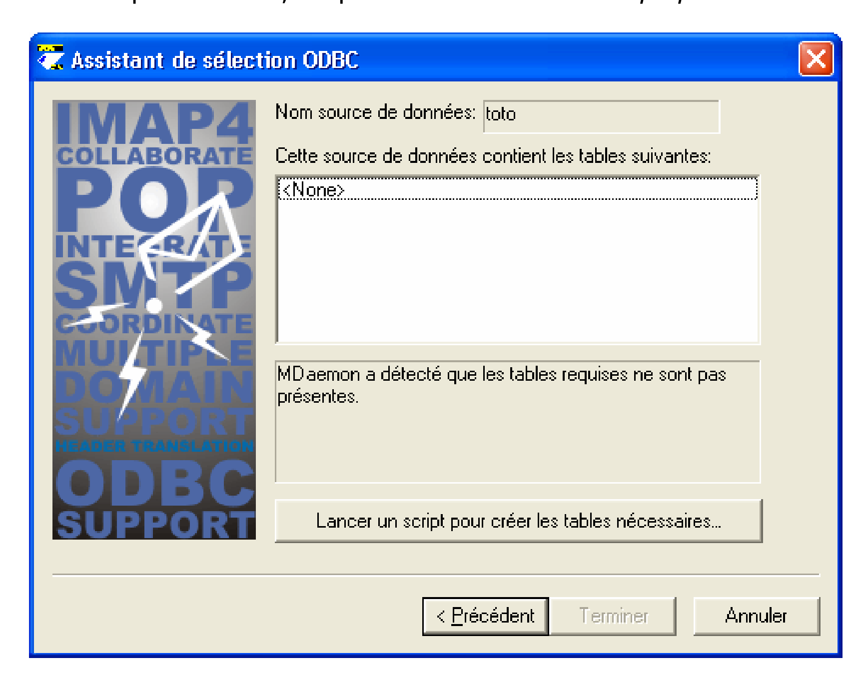


2. Sélectionnez la source de données que vous souhaitez utiliser pour votre base de données de comptes. Si aucune source de données système compatible n'est répertoriée, créez-en une nouvelle en suivant les instructions fournies dans **Création d'une nouvelle source de données ODBC** 362.

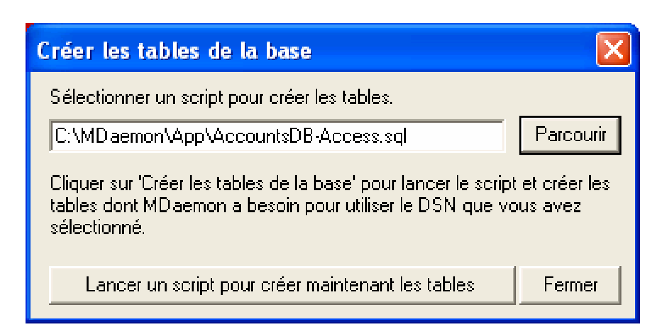
3. Si nécessaire, indiquez un identifiant et un mot de passe.

4. Cliquez sur Suivant.

5. If Si la source de données contient déjà les tables requises par MDaemon, passez à l'étape 8. Sinon, cliquez sur *Lancer un script pour créer les tables nécessaires…*



6. Saisissez le chemin (ou cliquez sur *Parcourir*) vers le fichier du script que vous souhaitez utiliser pour créer des tables dans votre application de base de données. Le dossier \MDaemon\app\ contient des scripts pour les applications de base de données les plus utilisées.



7. Cliquez sur *Lancer un script pour créer maintenant les tables*, puis sur *OK* et sur *Fermer*.

8. Cliquez sur *OK* pour fermer la boîte de dialogue *Base de données des comptes*.

9. Un outil de migration de base de données de comptes migrera tous les comptes de vos utilisateurs vers la source de données ODBC puis fermera MDaemon. Cliquez sur OK, puis redémarrez MDaemon. Vous pouvez commencer à utiliser la nouvelle base de données de comptes ODBC.

Voir également :

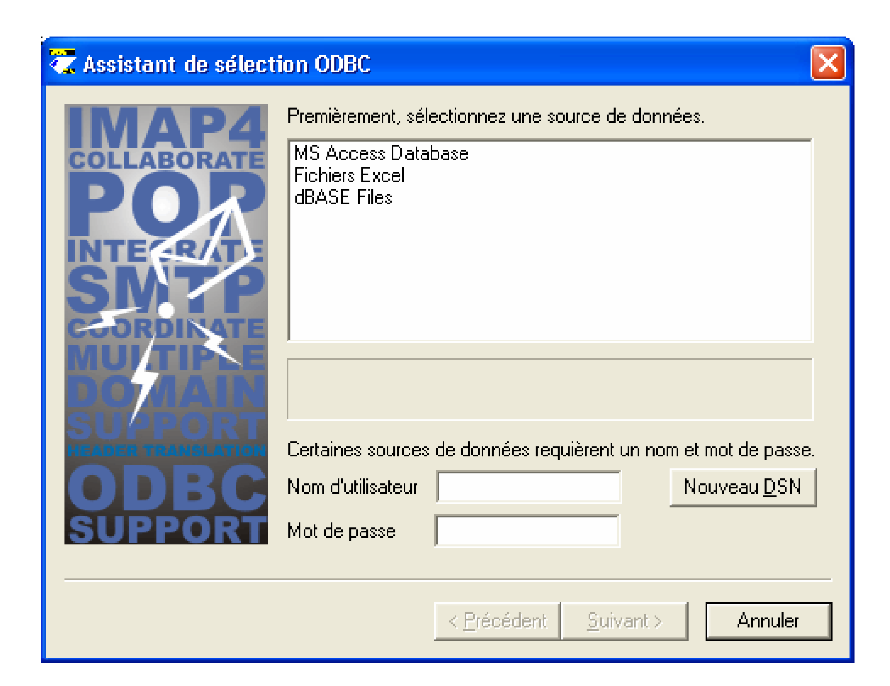
Base de données des comptes 359
Création d'une nouvelle source de données ODBC 362

5.2.6.1.1 Création d'une nouvelle source de données ODBC

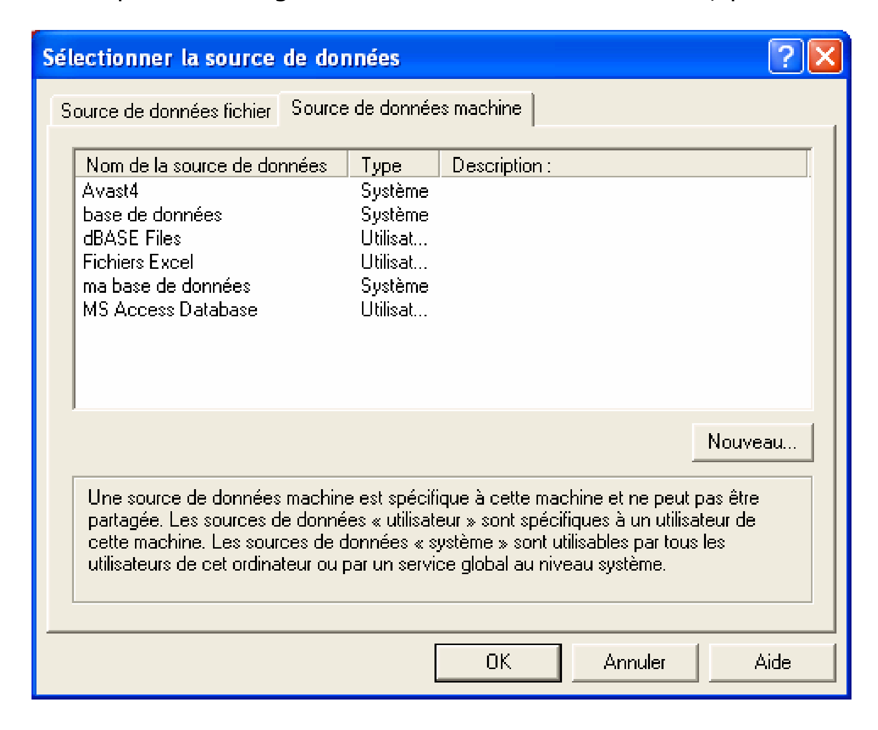
Pour créer une nouvelle source de données ODBC :

1. Dans Comptes » Paramètres des comptes » Base de données des comptes, sélectionnez l'option *Stocker les données de comptes dans une base de données ODBC accessible* puis cliquez sur *Configurer* pour ouvrir l'assistant.

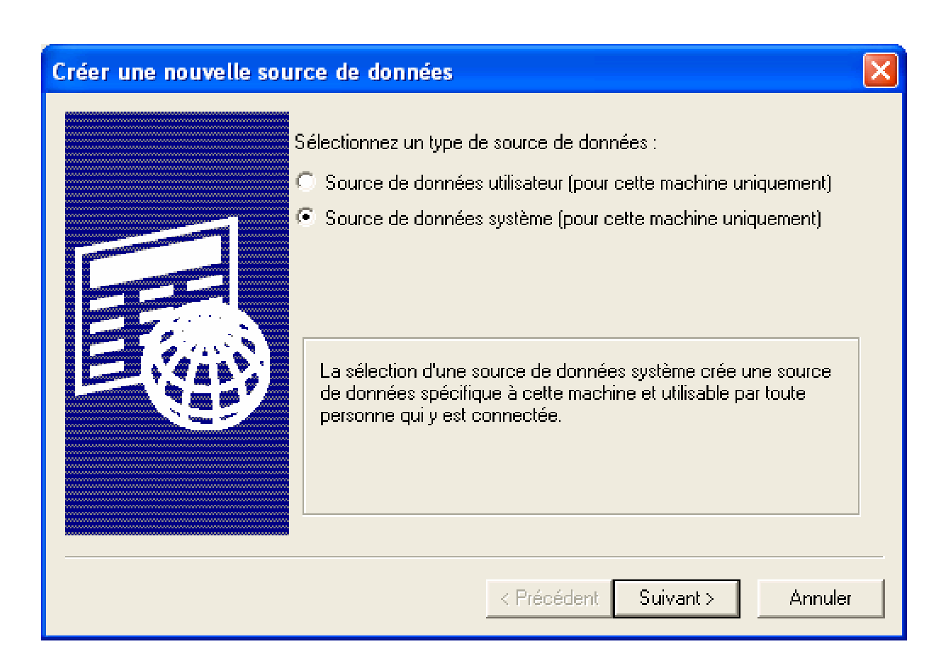
2. Cliquez sur *Nouveau DSN* pour ouvrir la boîte de dialogue *Sélectionner la source de données*.



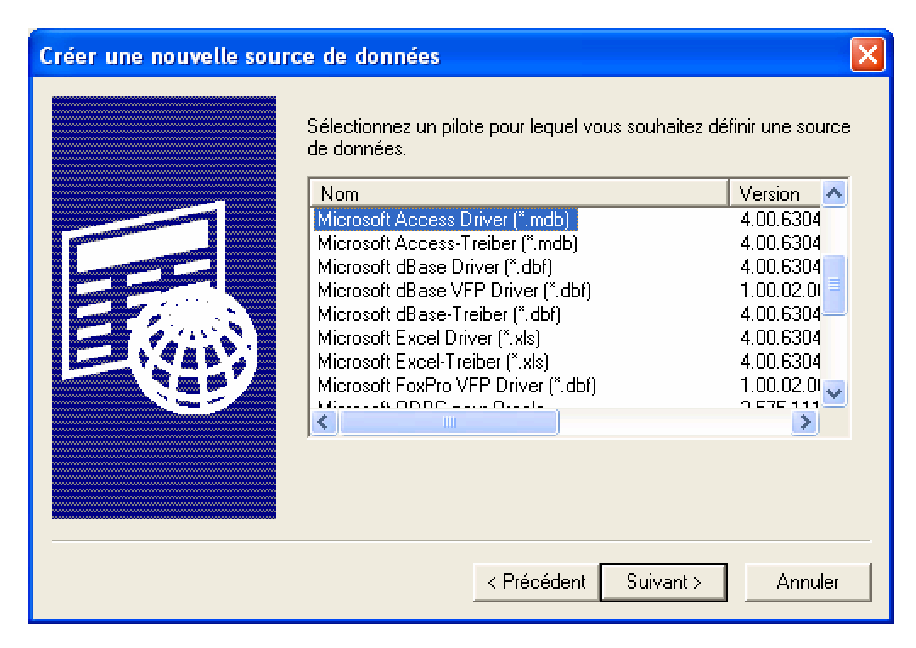
3. Cliquez sur l'onglet *Source de données machine*, puis sur *Nouveau*....



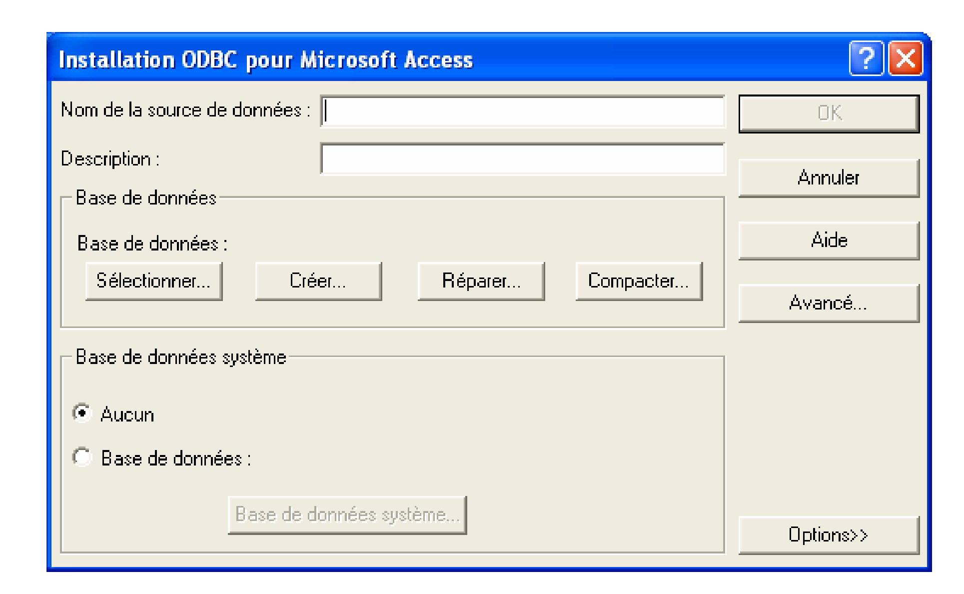
4. Sélectionnez *Source de données système*, puis cliquez sur Suivant.



5. Sélectionnez le pilote de base de données pour lequel vous souhaitez définir une source de données, puis cliquez sur *Suivant*.



6. Cliquez sur *Terminer* pour afficher la boîte de dialogue de configuration du pilote. Cette boîte de dialogue dépendra du pilote que vous avez sélectionné (ici : boîte de dialogue de configuration de Microsoft Access).



7. Indiquez un nom pour votre nouvelle source de données et fournissez les informations requises dans la boîte de dialogue du pilote (comme créer ou indiquer une base de données, choisir un répertoire ou un serveur, etc.).

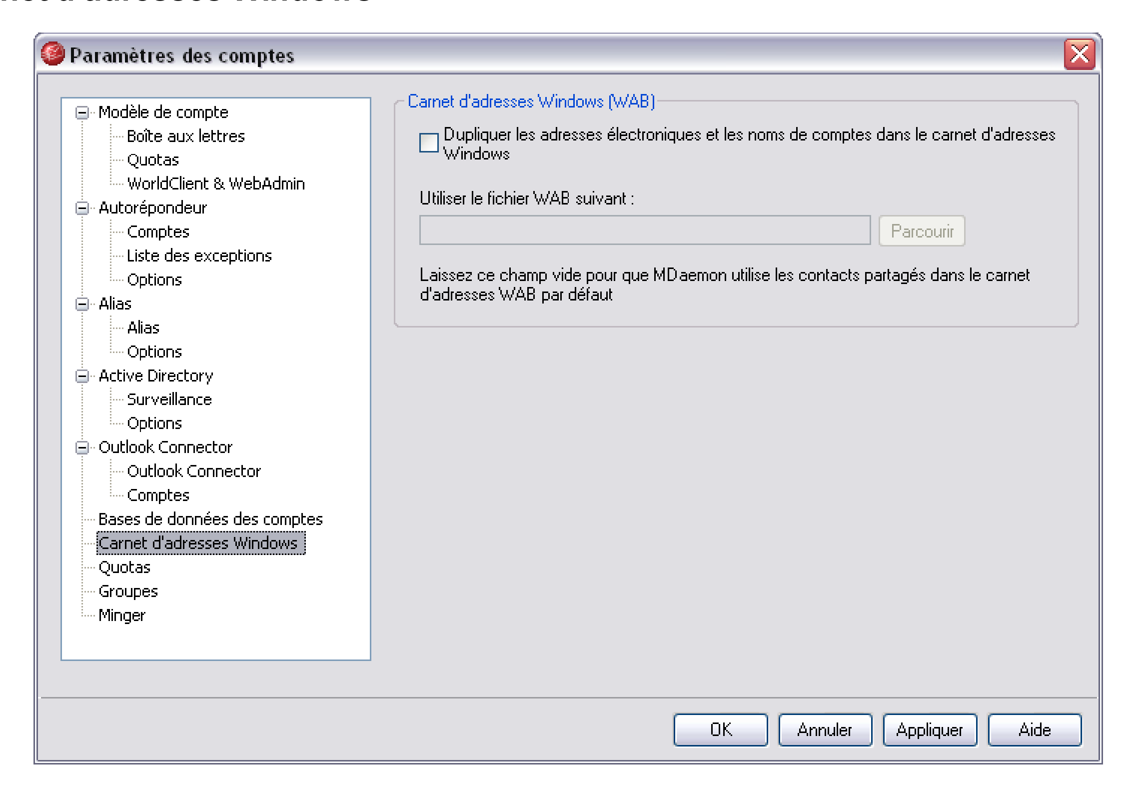
8. Cliquez sur *OK* pour fermer la boîte de dialogue du pilote.

9. Cliquez sur *OK* pour fermer la boîte de dialogue *Base de données des comptes*.

Voir également :

Base de données des comptes 359
Assistant de sélection ODBC 360

5.2.7 Carnet d'adresses Windows



MDaemon peut maintenir automatiquement à jour un fichier de Carnet d'adresses Windows (*.wab) ou Microsoft Outlook avec l'adresse électronique et le nom complet de chaque compte. Cela est souhaitable pour ceux qui souhaitent partager un carnet d'adresses avec des utilisateurs de produits comme Outlook, mais qui ne souhaitent pas utiliser un serveur LDAP ou ComAgent dans ce but.

Carnet d'adresses Windows (WAB)

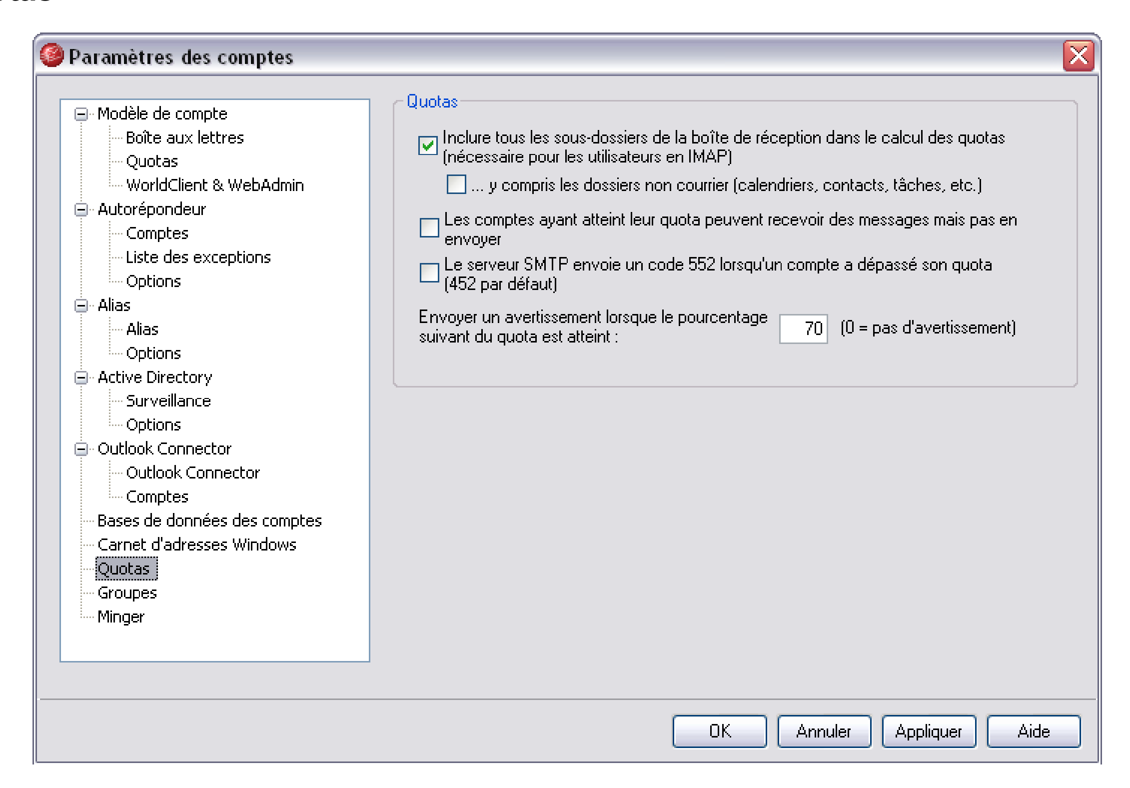
Dupliquer les adresses électroniques et noms de comptes dans le carnet d'adresses Windows

Activez cette option si vous voulez que les noms et les adresses électroniques de vos utilisateurs soient dupliqués dans un fichier *.wab ou dans le Carnet d'adresses Microsoft Outlook. Dans le Carnet d'adresses Windows, dans le menu Outils|Options, vous pouvez indiquer si votre carnet d'adresses Windows partagera les informations de contact avec Outlook et d'autres applications en stockant des données dans le Carnet d'adresses Microsoft Outlook ou dans un fichier de carnet d'adresses (*.wab).

Utiliser le fichier WAB suivant

Indiquez le chemin vers le fichier *.wab dans lequel vous souhaitez dupliquer les informations de vos utilisateurs. Si vous laissez cette commande vide, MDaemon utilisera alors les contacts partagés stockés dans le Carnet d'adresses Windows par défaut.

5.2.8 Quotas



Quotas

Inclure tous les sous-dossiers de la boîte de réception dans le calcul des quotas (nécessaire pour les utilisateurs en IMAP)
Lorsque cette case est cochée, tous les fichiers et les sous-dossiers dans la boîte de réception de l'utilisateur sont pris en compte lors de l'application des quotas. Sinon, seuls les véritables fichiers de messages sont pris en compte pour ces limitations.

...y compris les dossiers non courrier
Inclut tous les autres dossiers dans le calcul des quotas (calendrier, contacts, tâches...).

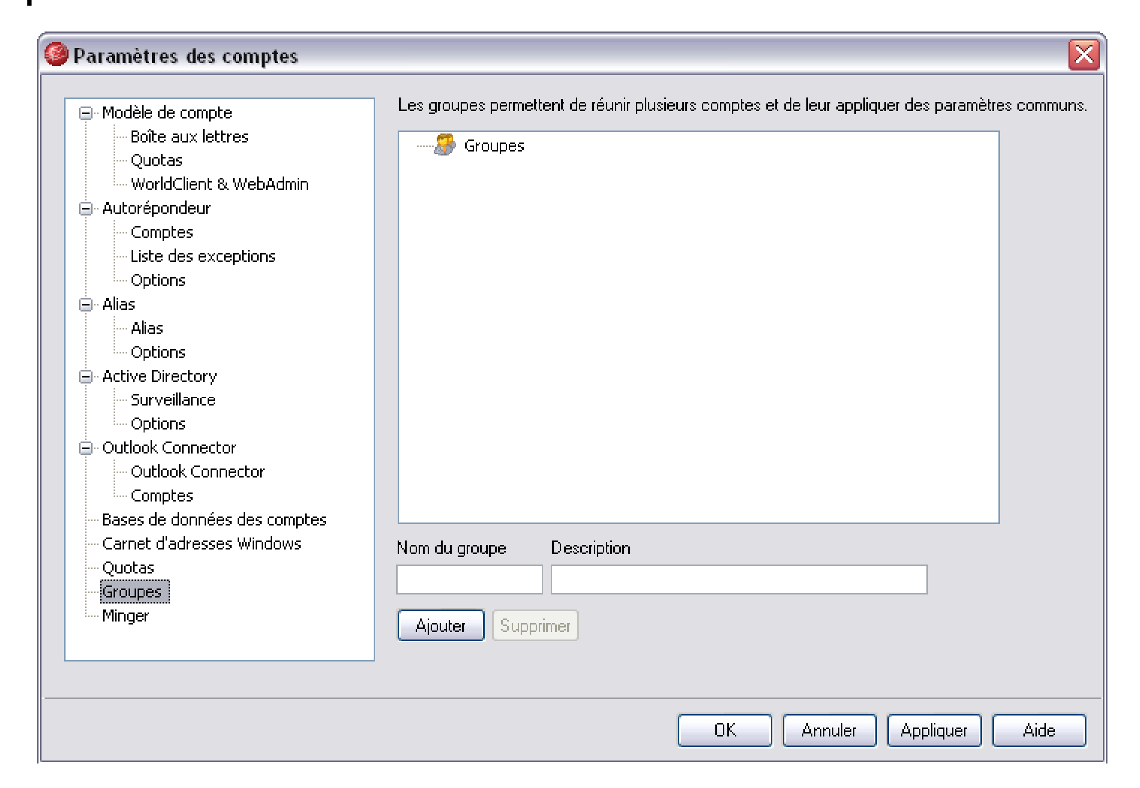
Les comptes ayant atteint leur quota peuvent recevoir des messages mais pas en envoyer
Normalement, lorsqu'un compte est limité en nombre de messages qu'il peut contenir, son titulaire ne peut plus recevoir de courrier lorsque le quota autorisé est dépassé. MDaemon n'acceptera plus aucun message pour ce compte tant que le titulaire n'en a pas supprimé certains. Cependant, l'utilisateur peut toujours envoyer du courrier si son compte dépasse le quota. Sélectionnez cette option pour la limitation agisse dans le sens opposé : lorsqu'un compte dépasse le quota, il peut toujours recevoir du courrier mais ne peut pas en envoyer.

Le serveur SMTP envoie un code 552 lorsqu'un compte a dépassé son quota (452 par défaut)
Par défaut, lorsqu'un compte a dépassé son quota MDaemon envoie le code d'erreur

temporaire 452 ("Requested action not taken: insufficient system storage") lors de la session SMTP. Cela signifie que le serveur expéditeur doit réessayer ultérieurement. Cochez cette case si vous souhaitez envoyer le code d'erreur permanente 552 ("Requested mail action aborted: exceeded storage allocation").

Envoyer un avertissement lorsque le pourcentage suivant du quota est atteint (0=pas d'avertissement)
Lorsqu'un compte excède le pourcentage indiqué du quota défini dans l'Éditeur de compte 317, un message d'avertissement lui est envoyé à minuit. Il contient le nombre de messages et l'espace utilisés, les quantités autorisées, ainsi que l'espace restant. De plus, si un message d'avertissement se trouve déjà dans la boîte aux lettres, il est remplacé par le nouveau. Indiquez "0" si vous souhaitez pas envoyer d'avertissements.

5.2.9 Groupes



Groupes

Cet onglet permet de créer des groupes d'utilisateurs. Il est possible d'ajouter un compte à un groupe depuis l'Éditeur de comptes 303, et de créer des règles 180 dans le Filtre de contenu en fonction de l'appartenance à un groupe. Les droits d'accès 70 aux Dossiers publics 64 peuvent également s'appliquer à des groupes d'utilisateurs.

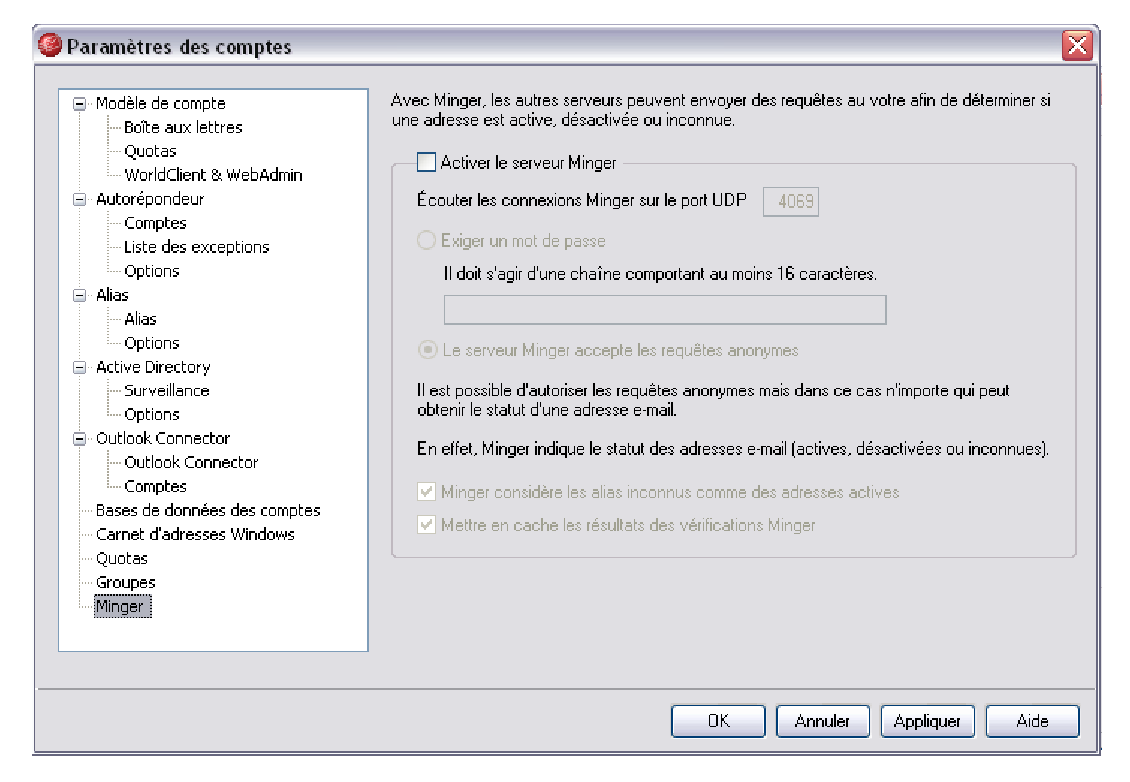
Nom du groupe
Nom du nouveau groupe.

Description
Indiquez dans ce champ une brève description.

Ajouter
Après avoir choisi un nom et une description, cliquez sur ce bouton pour ajouter le groupe à la liste.

Supprimer
Pour supprimer un groupe, sélectionnez-le et cliquez sur ce bouton.

5.2.10 Minger



Minger est un nouveau protocole de vérification des adresses créé par Alt-N Technologies. Basé initialement sur le protocole Finger, Minger fournit un système simple et efficace de vérification des adresses. Ce protocole est plus efficace que son prédécesseur car il utilise UDP et non TCP, et il est possible d'exiger une authentification. Les options de Minger sont disponibles en cliquant sur Comptes » Paramètres des comptes.

Le système de passerelles de MDaemon intègre également un client Minger (voir Vérification 409). Ainsi, lorsque MDaemon est utilisé en tant que passerelle il est possible de vérifier si les adresses des destinataires des messages sont correctes. Cela évite de devoir présumer que toutes les adresses sont valides.

Le dernier brouillon du protocole Minger est disponible à l'adresse ::

http://tools.ietf.org/html/draft-hathcock-minger-05

Serveur Minger

Activer le serveur Minger
Cochez cette case pour activer le serveur Minger de MDaemon.

Écouter les connexions Minger sur le port UDP
Port écouté par le serveur Minger. Les ports TCP et UDP 4069 sont réservés par l'IANA (Internet Assigned Numbers Authority) exclusivement pour les serveurs et clients Minger. Il est donc recommandé de conserver les numéros de port par défaut.

Exiger un mot de passe
Si vous souhaitez exiger une authentification par le biais d'un mot de passe, activez cette option et indiquez une chaîne comportant au moins 16 caractères. Lorsque cette option est activée, le serveur Minger refuse les requêtes non authentifiées.

Le serveur Minger accepte les requêtes anonymes
Cochez cette option pour accepter les requêtes non authentifiées. Les requêtes anonymes sont similaires aux actions pouvant être effectuées à l'aide de la commande SMTP VRFY ou SMTP "call back" ou "call forward", mais ces dernières sont plus efficaces. De plus, ces méthodes présentent de nombreux inconvénients.

Minger considère les alias inconnus comme des adresses actives
Lorsque cette option est activée, Minger considère les alias pointant vers des adresses externes comme des adresses actives connues. Ceci est obligatoire lorsqu'une requête provient de SecurityGateway, que cette option soit activée ou pas.

Mettre en cache les résultats des vérifications Minger
Par défaut, MDaemon conserve en cache les résultats des vérifications Minger. Désactivez cette option si vous ne souhaitez pas les conserver.

5.3 Import de comptes

5.3.1 Import de comptes depuis un fichier texte

Cliquez sur Comptes » Importer » Importer les comptes à partir d'un fichier texte délimité par des virgules... pour accéder à cette fonctionnalité. Vous pouvez également y accéder en cliquant sur le bouton *Importer* dans le Gestionnaire de comptes. C'est une méthode simple pour importer et générer automatiquement des comptes de messagerie. MDaemon lit le fichier texte et génère des nouveaux comptes de messagerie en n'utilisant que les noms et prénoms de l'utilisateur. Si vous configurez de manière efficace le Modèle de compte 330 vous pouvez générer des comptes uniques en n'utilisant que les noms et prénoms de vos utilisateurs. Mais vous pouvez également inclure de nombreuses autres options pour l'utilisateur indiqué si vous voulez remplacer

les valeurs par défaut. Tous les champs doivent être séparés par des virgules.

Chaque ligne du fichier texte délimité par des virgules ne doit contenir qu'une seule entrée. La première ligne doit être une ligne de base indiquant les noms et les séquences des champs dans les lignes suivantes. Un fichier d'exemple ressemble à ceci :

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"frank", "Frank Thomas", "C:\Mail\Frank\", N
```



MDaemon utilise les noms des champs de la ligne de base pour déterminer la séquence de données. Ces noms de champs peuvent donc apparaître dans n'importe quel ordre. Ils doivent être entre guillemets.

Toutes les chaînes doivent être entre guillemets et les valeurs booléennes sont considérées comme FAUSSES sauf si le premier caractère est y, Y, 1, t, or T.

Les prénoms et noms peuvent figurer dans le nom complet. Toutefois, n'y insérez pas de virgules.

Après avoir effectué le traitement de l'importation, MDaemon crée TXIMPORT.LOG, qui détaille les résultats de l'importation et répertorie les comptes importés avec succès et ceux dont l'importation a échoué. La raison principale pour laquelle un compte ne peut pas être importé résulte d'un conflit avec une boîte aux lettres, un nom ou des informations du dossier d'un compte existant, d'un conflit avec un alias existant, ou d'un conflit avec le nom d'une liste de diffusion.

Voir la description de MD_ImportUserInfo() et de MD_ExportAllUsers() dans le fichier MD-API.HTML situé dans votre répertoire \API\, pour obtenir plus d'informations sur le mappage de champs.

Utilisez les valeurs suivantes pour le mappage avec les champs de comptes MDaemon :

Nom du champ	Type
MailBox	chaîne
Domain	chaîne
FullName	chaîne
MailDir	chaîne
Password	chaîne
AutoDecode	booléen
IsForwarding	booléen
AllowAccess	booléen

AllowChangeViaEmail	booléen
KeepForwardedMail	booléen
HideFromEveryone	booléen
EncryptMail	booléen
ApplyQuotas	booléen
EnableMultiPOP	booléen
MaxMessageCount	nombre entier
MaxDiskSpace	nombre entier
FwdAddress	chaîne
FwdHost	chaîne
FwdSendAs	chaîne
FwdPort	chaîne
NTAccount	chaîne
MailFormat	chaîne
AutoRespScript	chaîne
AutoRespProcess	chaîne
AddToList	chaîne
RemoveFromList	chaîne
PassMessageToProcess	booléen
MaxUIDLCount	nombre entier
MaxMessageSize	nombre entier
RecurseIMAP	booléen
MaxInactive	nombre entier
MaxMessageAge	nombre entier
MaxDeletedIMAPMessageAge	nombre entier
Comments	chaîne
UserDefined	chaîne

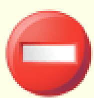
Voir également :

Intégration des comptes Windows 372

5.3.2 Intégration des comptes Windows

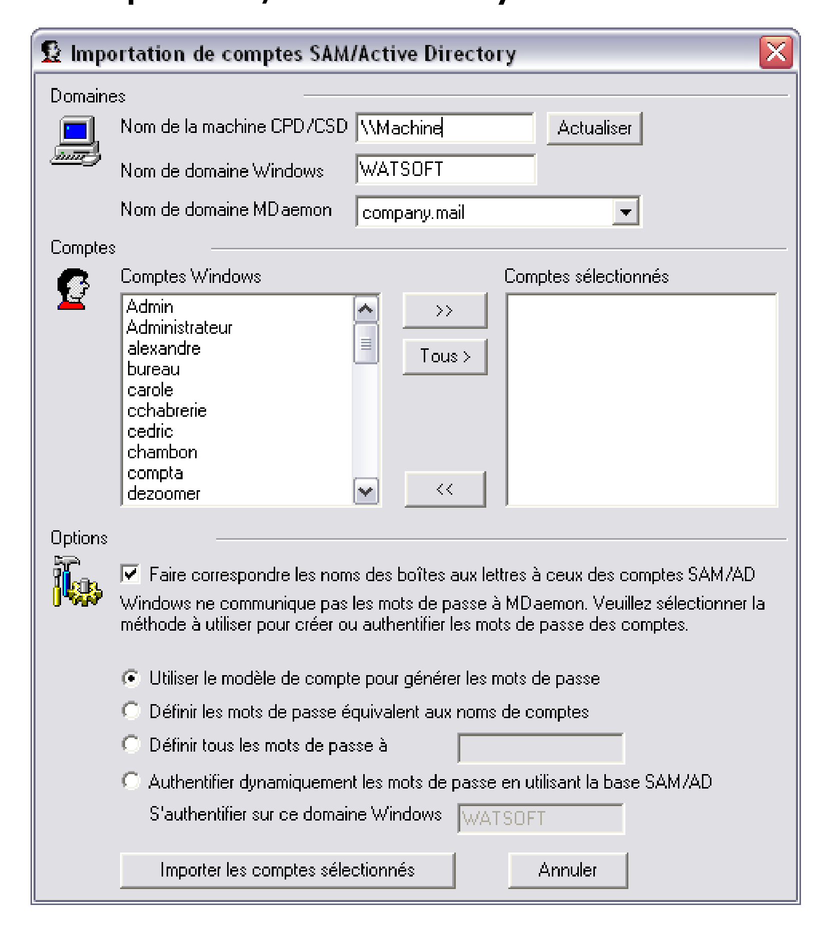
MDaemon supporte l'intégration de comptes Windows. Cela consiste en un moteur d'importation de base de données utilisateur SAM/Active Directory qui se trouve dans Comptes » Importer » Importer les comptes à partir de la base SAM/Active Directory . De plus, la prise en charge de l'authentification dynamique d'utilisateurs est intégrée

au code de gestion des utilisateurs de MDaemon. Il est possible d'indiquer un domaine Windows dans le champ mot de passe d'un compte pour que MDaemon authentifie dynamiquement ce type de compte en temps réel à l'aide du système de sécurité du domaine Windows indiqué. Ainsi, en modifiant le mot de passe du compte dans Windows, MDaemon est automatiquement mis à jour. Par conséquent, vos utilisateurs n'auront à mémoriser qu'une référence d'authentification. Cela permet également de configurer très facilement des comptes pour de nouvelles installations.



Le contexte de sécurité du compte exécutant MDaemon doit disposer du privilège SE_TCB_NAME. Si le processus est un service exécuté avec le compte Système local, il dispose par défaut de ce privilège. Sinon, il doit être défini dans la gestion des utilisateurs Windows pour le compte avec lequel MDaemon est exécuté.

Importation de comptes SAM/Active Directory



Domaines

Nom de la machine CPD/CSD
Ce champ vous permet d'indiquer le nom de l'ordinateur à partir duquel MDaemon lit les informations de la base de données de comptes Windows. Vous pouvez indiquer \\<DEFAULT> pour que MDaemon lise les données depuis l'ordinateur local.

Actualiser
Cliquez sur ce bouton pour actualiser la liste des comptes Windows.

Nom de domaine Windows
Indiquez le nom de domaine Windows à partir duquel vous souhaitez importer des comptes.

Nom de domaine MDaemon
Sélectionnez dans la liste de choix le domaine MDaemon dans lequel les comptes seront importés.

Comptes

Comptes Windows
Cette fenêtre contient une liste de tous les comptes collectés depuis la base de données de comptes Windows.

Comptes sélectionnés
Cette fenêtre contient tous les comptes que vous avez sélectionnés et que vous souhaitez importer.

>>
Cliquez sur ce bouton pour déplacer les comptes surlignés de "Comptes Windows" vers "Comptes sélectionnés".

<<
Cliquez sur ce bouton pour retirer les entrées surlignées de la liste "Comptes sélectionnés".

Options

Faire correspondre les noms des boîtes aux lettres à ceux des comptes SAM/AD
Activez ce paramètre pour que chaque nom de compte d'utilisateur Windows importé soit utilisé comme valeur de leur boîte aux lettres. Grâce à cette méthode, vous n'aurez pas à configurer de macros dans le Modèle de compte.

Utiliser le modèle de compte pour générer les mots de passe
Avec cette option, MDaemon génère des mots de passe pour les comptes importés à l'aide des paramètres du Modèle de compte[330].

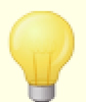
Définir les mots de passe équivalents aux noms des comptes
Avec cette option, MDaemon utilise le nom de compte comme mot de passe.

Définir tous les mots de passe à
Ce paramètre vous permet d'indiquer un mot de passe unique qui sera utilisé par tous les comptes importés.

Authentifier les mots de passe dynamiquement en utilisant la base SAM/AD
Ce paramètre active l'authentification dynamique des comptes importés. Plutôt que d'indiquer un mot de passe, MDaemon authentifie simplement les valeurs USER et

PASS fournies par le client de messagerie à l'aide de la base de données Windows en temps réel.

S'authentifier sur ce domaine Windows
Entrez le nom du domaine Windows que MDaemon utilisera lors de l'authentification dynamique de connexions. **Il ne s'agit pas du nom de l'ordinateur du contrôleur du domaine, mais du nom réel du domaine Windows.**



Lorsque des comptes sont configurés avec une authentification dynamique, le nom du domaine Windows, précédé par deux barres obliques inverses, est utilisé dans le champ Mot de passe du compte. Il est stocké sous forme non cryptée dans le fichier USERLIST.DAT. Par exemple, si un compte est configuré avec une authentification dynamique sur un domaine Windows appelé ALTN, le champ Mot de passe contiendra la valeur \\ALTN. Les deux barres obliques inverses qui précèdent le nom de domaine indiquent que le champ Mot de passe contient le nom d'un domaine Windows et que MDaemon authentifie les valeurs USER et PASS fournies par le client de messagerie en s'appuyant sur la base de données du compte. Si le compte n'est pas configuré avec une authentification dynamique, le mot de passe ne doit pas être précédé de deux barres obliques inverses.

Vous pouvez saisir deux barres obliques inverses et le nom de domaine Windows dans le champ mot de passe d'un compte en utilisant l'Éditeur de compte 301. L'administrateur n'est pas obligé d'utiliser l'outil d'importation pour configurer les comptes avec l'authentification dynamique.

Voir également :

Import de comptes depuis un fichier texte 370
Éditeur de compte » Compte 301



Section VI

6 Menu Listes

6.1 Listes de diffusion

Les listes de diffusion, appelées parfois Listes de distribution, permettent d'envoyer des messages à des groupes d'utilisateurs comme s'ils partageaient une boîte aux lettres commune. Des copies des messages envoyés à la liste sont distribuées à chaque membre de la liste. Les listes peuvent contenir des membres avec des adresses locales et/ou distantes, peuvent être publiques ou privées, modérées ou ouvertes, envoyées en format compilation ou en format normal, etc.

Éditeur de liste de diffusion

L'Éditeur de liste de diffusion permet de créer et modifer des listes. Pour y accéder, cliquez sur Listes » Nouvelle liste de diffusion... ou Listes » Modifier une liste de diffusion. Il contient les onglets suivants :

Paramètres 379
Membres 381
Inscription 384
Modération 387
Compilation 388
Routage 390
Notifications 391
Fichiers de support 392
Dossier public 394
Active Directory 395
ODBC 397

Créer une nouvelle liste de diffusion

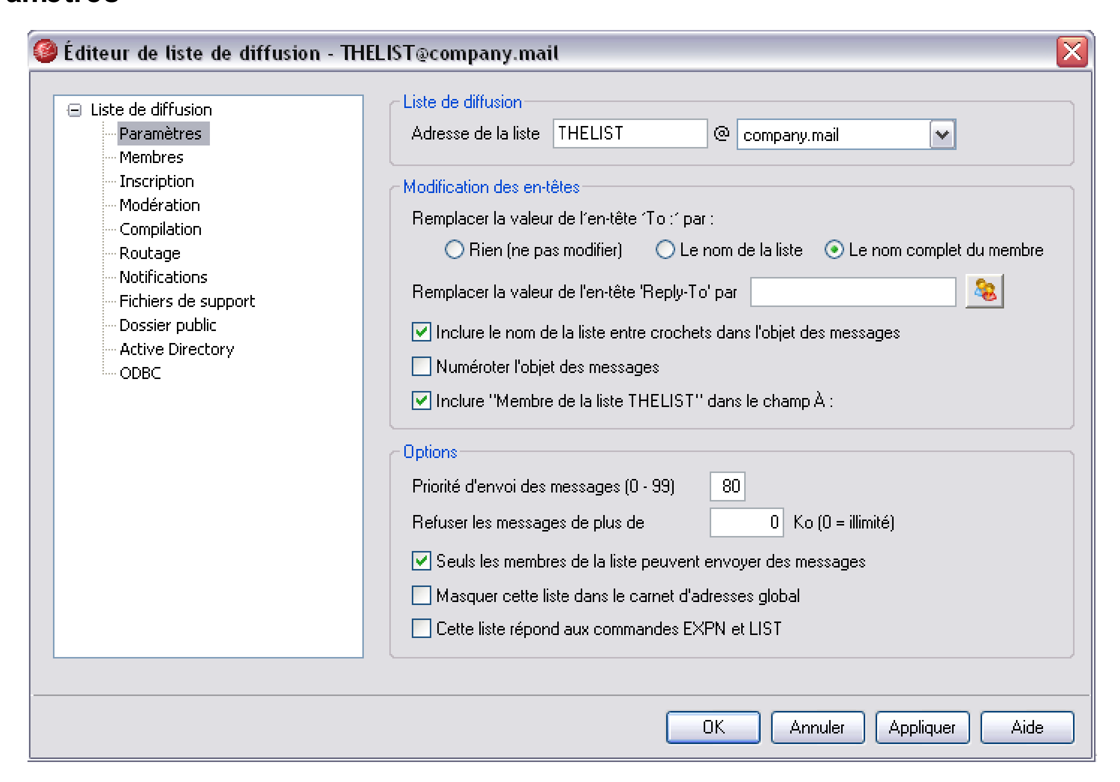
Cliquez sur Listes » Nouvelle liste de diffusion. L'Éditeur de liste de diffusion s'ouvre pour vous permettre de créer une nouvelle liste. Pour la créer, vous n'avez qu'à donner un nom à la liste et indiquer le domaine auquel elle appartient. Toutes les autres options contiennent des paramètres par défaut. Vous pouvez modifier ces paramètres lors de la création de la liste ou les modifier plus tard.

Modifier une liste de diffusion existante

Cliquez sur Listes » Modifier une liste de diffusion pour ouvrir la boîte de dialogue Sélectionner liste de diffusion. Cette boîte de dialogue sert à choisir la liste de diffusion que vous souhaitez modifier. Lorsqu'une liste est sélectionnée dans cette boîte de dialogue, elle s'ouvre dans l'éditeur de Liste de diffusion afin de consulter ou modifier ses paramètres.

6.1.1 Éditeur de liste de diffusion

6.1.1.1 Paramètres



Liste de diffusion

Adresse de la liste
Indiquez un nom pour la liste de diffusion, puis sélectionnez le domaine auquel elle appartient dans le menu déroulant. Les messages destinés à la liste utiliseront le nom et le domaine indiqués ici (par exemple : maliste@mondomaine.com). Les noms de liste ne peuvent pas contenir les caractères "!" ou "|".

Adresse de retour
Tapez l'adresse e-mail à laquelle vous voulez que les réponses à la liste soient destinées ou cliquez sur l'icône pour en sélectionner une. Entrez l'adresse de la liste si vous voulez que les réponses soient renvoyées à la liste. Si vous laissez ce champ vide, les réponses aux messages de la liste seront redirigées vers l'expéditeur du message.

Modification des en-têtes

Remplacer la valeur de l'en-tête 'TO:' par :
Utilisez ces options pour indiquer l'adresse contenue dans l'en-tête TO: lorsque MDaemon reçoit un message destiné à la liste.

Rien (ne pas modifier) - MDaemon n'effectue pas de modifications dans l'adresse affichée. L'adresse de l'en-tête TO: correspond exactement à la valeur saisie par 'lexpéditeur du message.

Le nom de la liste - Insère l'adresse de la liste de diffusion dans l'en-tête TO:.

Le nom complet du membre - Insère dans l'en-tête TO: l'adresse du membre de la liste à qui le message est destiné.



L'option *Nom complet du membre* ne peut être sélectionnée que si l'option *Distribuer le courrier individuellement à chaque membre* est sélectionnée dans l'onglet Routage390. Si vous avez sélectionné *Distribuer le courrier en utilisant une commande RCPT pour chaque membre*, MDaemon insère par défaut l'adresse de la liste.

Remplacer la valeur de l'en-tête 'Reply-To' par
Saisissez l'adresse e-mail à laquelle vous souhaitez que les réponses soient envoyées, ou bien cliquez sur l'icône pour sélectionner un compte. Si vous souhaitez que les réponses soient envoyées à la liste, indiquez l'adresse de la liste. Si vous laissez ce champ vide, les réponses seront envoyées à l'expéditeur du message. En règle générale, les réponses sont envoyées à la liste plutôt qu'à l'expéditeur du message.

Inclure le nom de la liste entre crochets dans l'objet des messages
Avec cette, MDaemon ajoute le nom de la liste entre crochets (par exemple : [MaListe]) au début de l'objet dans tous les messages envoyés à la liste.

Numéroter l'objet des messages
Cette option permet d'insérer un numéro dans l'objet des messages envoyés à la liste. Les numéros sont ajoutés à la fin de l'objet. En classant les messages de votre boîte de réception par objet, le courrier de la liste s'affiche dans l'ordre chronologique.

Inclure 'Membre de la liste XX' dans le champ A:
Lorsque cette option est activée, le texte "Membre la liste [nom de la liste]" est inséré dans la portion "nom réel" du champ A.



Tous les clients de messagerie ne prennent pas en charge l'affichage des "noms réels" dans le champ À: des messages. Dans ces clients de messagerie, seules les adresses électroniques réelles indiquées dans l'option *Remplacer la valeur de l'en-tête 'TO:' par* s'affichent.

Options

Priorité d'envoi des messages (0-99)
Saisissez un nombre compris entre 0 et 99 dans ce champ. Cette valeur indique l'ordre de priorité des messages lors de la distribution. Plus la valeur est basse, plus le message est considéré comme important et plus il sera prioritaire dans la file d'attente de messages. Pour indication : 10 = Urgent, 50 = Normal et 80 = Envoi en masse.

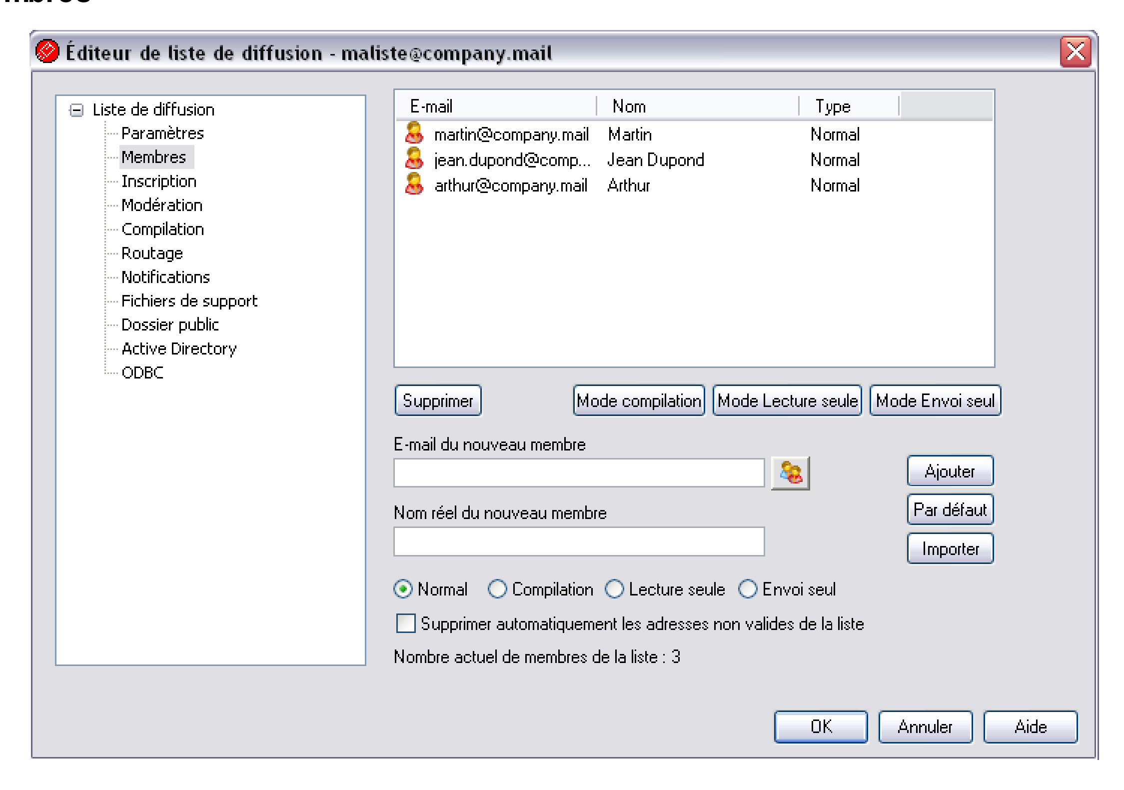
Refuser les messages de plus de [xx] Ko
Cette option permet d'indiquer une limite de taille pour les messages destinés à la liste de diffusion. Les messages dépassant cette limite sont refusés.

Seuls les membres de la liste peuvent envoyer des messages
Lorsque cette option est activée, la liste est considérée comme "privée" : seuls les membres peuvent envoyer des messages. Les messages provenant de personnes n'étant pas membres sont refusés.

Masquer cette liste dans le carnet d'adresses global
Sélectionnez cette option pour masquer la liste de diffusion dans WorldClient et les carnets d'adresses LDAP publics.

Cette liste répond aux commandes EXPN et LIST
Si vous avez sélectionné cette option, l'adhésion à la liste sera indiquée en réponse à la commande EXPN ou LIST lors d'une session de messagerie. Sinon, cette information n'est pas transmise.

6.1.1.2 Membres



Cet onglet affiche l'adresse e-mail et le nom de tous les membres de la liste. Le "droit d'accès" (type) est également indiqué : normal, compilation, lecture seule ou envoi seul.

Supprimer
Pour supprimer un membre de la liste, sélectionnez-le et cliquez sur ce bouton.

Mode compilation
Sélectionnez un membre, puis cliquez sur ce bouton pour passer en mode Compilation 388.

Mode Lecture seule
Sélectionnez un membre, puis cliquez sur ce bouton pour le passer en mode "Lecture seule". Il recevra toujours les messages de la liste mais ne pourra plus lui en envoyer.

Mode Envoi seul
Sélectionnez un membre, puis cliquez sur ce bouton pour le passer en mode "Envoi seul". Il pourra envoyer des messages à la liste mais ne recevra pas les messages de la liste.

Ajout de membres

E-mail du nouveau membre
Saisissez l'adresse électronique que vous souhaitez ajouter à la liste de diffusion ou cliquez sur l'icône pour en rechercher une. Les adresses des membres ne peuvent pas contenir de caractères "!" ou "|".

Nom réel du nouveau membre
Saisissez le nom du membre. Ce nom figure dans l'en-tête "To:" des messages de la liste lorsque l'option *Remplacer la valeur de l'en-tête 'TO:' par : le nom complet du membre* est sélectionnée dans l'onglet Paramètres 379.

Normal, Compilation Lecture seule, Envoi seul
Sélectionnez le droit que vous souhaitez accorder au nouveau memebre.

Ajouter
Cliquez sur ce bouton pour ajouter le nouveau membre à la liste.

Par défaut
Pour définir un droit par défaut pour les nouveaux memebres (Normal, Compilation, Lecture seule, Envoi seul), sélectionnnez-le et cliquez sur ce bouton.

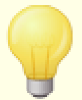
Importer
Cliquez sur ce bouton pour importer des membres depuis un fichier texte délimité par des virgules. Vous devez indiquer une entrée par ligne et tous les champs doivent être séparés par des virgules. De plus, la première ligne du fichier doit répertorier les noms des champs et l'ordre dans lequel ils apparaissent. Un des champs doit se nommer "Email" et contenir les adresses électroniques. Vous pouvez avoir un champ optionnel nommé "FullName" et contenant le nom du membre de la liste. Tous les autres champs seront ignorés par l'utilitaire d'import.

Par exemple :

```
"Email", "FullName", "Address", "telephone"
"frank@altn.com", "Frank Thomas", "123 Frank St", "817.555.1234"
```

Les membres importés ne reçoivent pas le message de bienvenue à la liste (s'il y en a un), et l'utilitaire d'import ne vérifie pas les doublons.

Supprimer automatiquement les adresses non valides de la liste
Lorsque cette option est activée, MDaemon supprime automatiquement une adresse de la liste lorsqu'il est rencontre à une erreur fatale permanente quand il tente de lui distribuer un message. Les adresses seront également considérées comme "non valides" et supprimées lorsque leurs messages sont déplacés vers le système de renvoi et qu'ils expirent par la suite dans le système.



Cette option sert en cas de refus des messages par le serveur distant. Elle ne peut être activée que si l'option *Distribuer le courrier individuellement à chaque membre* est sélectionnée dans l'onglet Routage 390. Si vous dirigez des messages de liste vers un hôte relais, consultez Amélioration du nettoyage de liste ci-dessous pour plus d'informations.

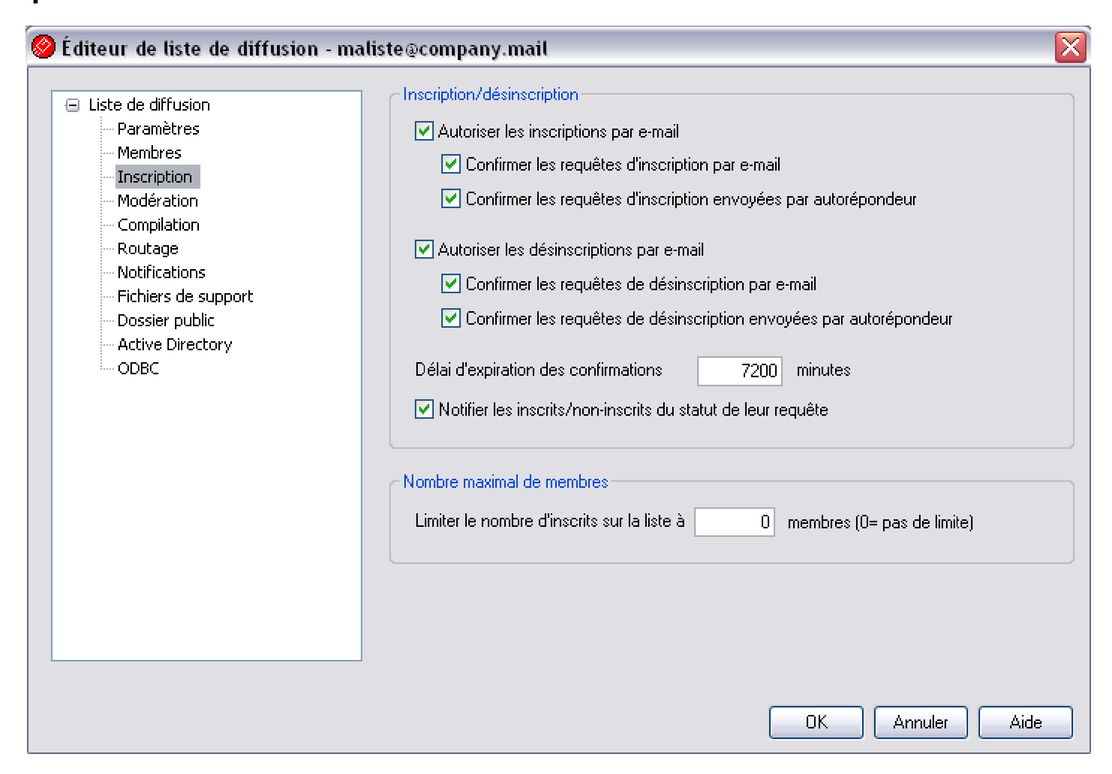
Nombre actuel de membres de la liste :
Affiche le nombre de membres actuellement inscrits à la liste de diffusion.

Amélioration du nettoyage de liste

Lorsque l'option *Supprimer automatiquement les adresses non valides de la liste* est activée et que vous avez indiqué une boîte aux lettres locale comme adresse SMTP 'Bounce' dans l'onglet Notifications 391, chaque jour à minuit MDaemon tente d'analyser les adresses posant des problèmes dans le courrier retourné et supprime les membres qui ne peuvent être atteints. Cela permet un nettoyage plus efficace des adresses invalides des listes de diffusion, particulièrement lorsque vous acheminez des messages de la liste vers un hôte relais plutôt que de les distribuer directement.

Dans Préférences » Divers 167 se trouvent deux options liées à cette fonctionnalité : *Le nettoyeur de liste supprime les messages qui comportent des adresses inanalysables* et *Le nettoyeur de liste sauvegarde les messages des membres supprimés d'une liste*.

6.1.1.3 Inscription



Inscription/désinscription

Autoriser les inscriptions par e-mail
Lorsque cette option est activée, les utilisateurs peuvent s'inscrire en envoyant des requêtes, à l'aide de messages spécialement formatés ou d'autorépondeurs. Pour en savoir plus, voir : Inscription aux listes de diffusion 385.

Confirmer les requêtes d'inscription par e-mail
Lorsque cette option est activée, MDaemon tente d’authentifier les requêtes d’inscription. Pour cela il envoie à l'adresse souhaitant s'inscrire un message contenant un "code" spécifique. Lorsque l'utilisateur répond à ce message, MDaemon l'ajoute à la liste de diffusion. Attention : la réponse doit être envoyée dans le délai indiqué ci-dessous.

Confirmer les requêtes d'inscription envoyées par autorépondeur
Cette option fonctionne de façon similaire à la précédente, mais elle s'applique aux requêtes d'inscription envoyées avec un Autorépondeur 310.

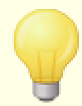
Autoriser les désinscriptions par e-mail
Lorsque cette option est activée, les utilisateurs peuvent se désinscrire en envoyant des requêtes, à l'aide de messages spécialement formatés ou d'autorépondeurs. Pour en savoir plus, voir : Inscription aux listes de diffusion 385.

Confirmer les requêtes de désinscription par e-mail
Lorsque cette option est activée, MDaemon tente d’authentifier les requêtes de désinscription. Pour cela il envoie à l'adresse souhaitant se désinscrire un

message contenant un "code" spécifique. Lorsque l'utilisateur répond à ce message, MDaemon le supprime de la liste de diffusion. Attention : la réponse doit être envoyée dans le délai indiqué ci-dessous.

Confirmer les requêtes de désinscription envoyées par autorépondeur
Cette option fonctionne de façon similaire à la précédente, mais elle s'applique aux requêtes de désinscription envoyées avec un Autorépondeur310.

Délai d'expiration des confirmations [XX] minutes
Lorsque MDaemon envoie un message pour confirmer les requêtes d'inscription ou de désinscription, l'utilisateur doit répondre avant la fin du délai indiqué ici. Si la réponse est envoyée après la fin du délai, la requête est ignorée et l'utilisateur doit en envoyer une nouvelle. Paramètre par défaut : 7200 minutes (5 jours).

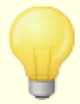


Cette valeur est globale : elle s'applique à toutes les listes de diffusion.

Notifier les inscrits/non inscrits du statut de leur requête
Lorsque cette option est activée MDaemon envoie un message de confirmation aux utilisateurs s'étant inscrits/désinscrits de la liste.

Nombre maximal de membres

Limiter le nombre d'inscrits sur la liste à [xx] membres (0=pas de limite)
Avec cette fonctionnalité, vous pouvez indiquer un nombre maximal de membres qui peuvent s'inscrire à la liste de diffusion. Entrez zéro dans ce champ si vous ne souhaitez pas limiter les inscriptions à la liste.



Cette limite ne concerne que les utilisateurs s'inscrivant par e-mail à l'aide des méthodes indiquées dans Inscription aux listes de diffusion385. Elle ne s'applique pas aux adresses ajoutées manuellement, ni aux requêtes envoyées par e-mail et contenant le mot de passe de la liste387.

Voir également:

Inscription aux listes de diffusion 385
Autorépondeur 310

6.1.1.3.1 Inscription aux listes de diffusion

Inscription/désinscription par e-mail

Pour s'inscrire à une liste de diffusion, envoyez un message à l'adresse MDaemon (ou un alias de cette adresse) sur le domaine hébergeant la liste de diffusion, et placez la commande Subscribe en première ligne du corps du message. Par exemple, il existe une

liste de diffusion appelée MDSupport et hébergée sur altn.com. Vous pouvez vous inscrire à cette liste en envoyant un message à "mdaemon@altn.com" et en saisissant SUBSCRIBE MDSupport@altn.com comme première ligne du corps du message. L'objet du message n'a pas d'importance et peut être vide.

Pour en savoir plus sur ce type de messages, voir : Contrôle du serveur à distance par e-mail 452.



Parfois, les utilisateurs tentent de s'inscrire/se désinscrire de listes en envoyant des messages directement à l'adresse de la liste plutôt qu'au compte système MDaemon. Le message est alors envoyé normalement aux membres de la liste et l'utilisateur n'est pas inscrit ou désinscrit. Pour éviter l'envoi de ce type de messages à des listes de diffusion, activez l'option *Rechercher le contenu inapproprié dans les messages destinés aux listes de diffusion* dans Configuration » Préférences » Système 159.

Inscription/désinscription à l'aide d'adresses spécifiques

Lorsque l'option *Répondre aux requêtes'<Liste>-subscribe' et '<Liste>-unsubscribe'* est activée (dans Configuration » Préférences » Divers 167) les utilisateurs peuvent également s'inscrire ou se désinscrire en envoyant un message à l'adresse de la liste suivie de "-subscribe" ou "-unsubscribe". Par exemple, si l'adresse de la liste est "franks-list@exemple.com", les utilisateurs peuvent s'inscrire envoyant un message à "franks-list-subscribe@exemple.com." De même, pour se désinscrire il suffit d'envoyer un message à "franks-list-unsubscribe@exemple.com." Le contenu du sujet et le corps du message n'ont pas d'importance. Ainsi, lorsque cette fonctionnalité est activée, MDaemon insère l'en-tête suivant dans tous les messages de la liste :

```
List-Unsubscribe: <mailto:<Liste>-Unsubscribe@domaine.com>
```

Certains clients de messagerie peuvent l'utiliser et mettre automatiquement un bouton Désinscription à la disposition des utilisateurs.

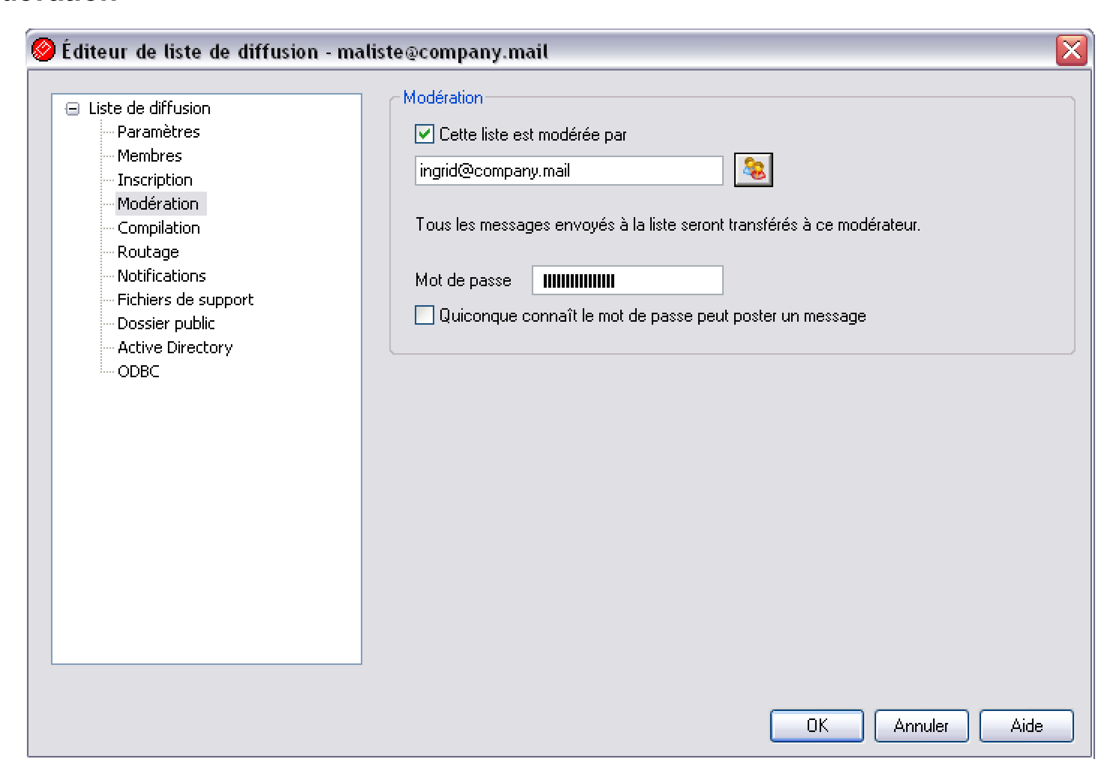
Inscription/désinscription par e-mail

Vous pouvez également utiliser un Autorépondeur 310 pour ajouter ou supprimer des membres. Pour cela, créez un ou plusieurs comptes MDaemon destinés uniquement à ajouter/supprimer des adresses lorsque des messages leur sont envoyés. Par exemple, si vous possédez une liste appelée "maliste@exemple.com" vous pouvez créer le compte : "rejoindre-maliste@exemple.com" et configurer un autorépondeur pour ce compte de façon à ajouter à la liste tous les utilisateurs envoyant un message à "rejoindre-maliste@exemple.com".

Voir également :

[Inscription](384)
[Contrôle du serveur à distance par e-mail](452)
[Autorépondeur](310)
[Préférences » Système](159)
[Préférences » Divers](167)

6.1.1.4 Modération



Modération

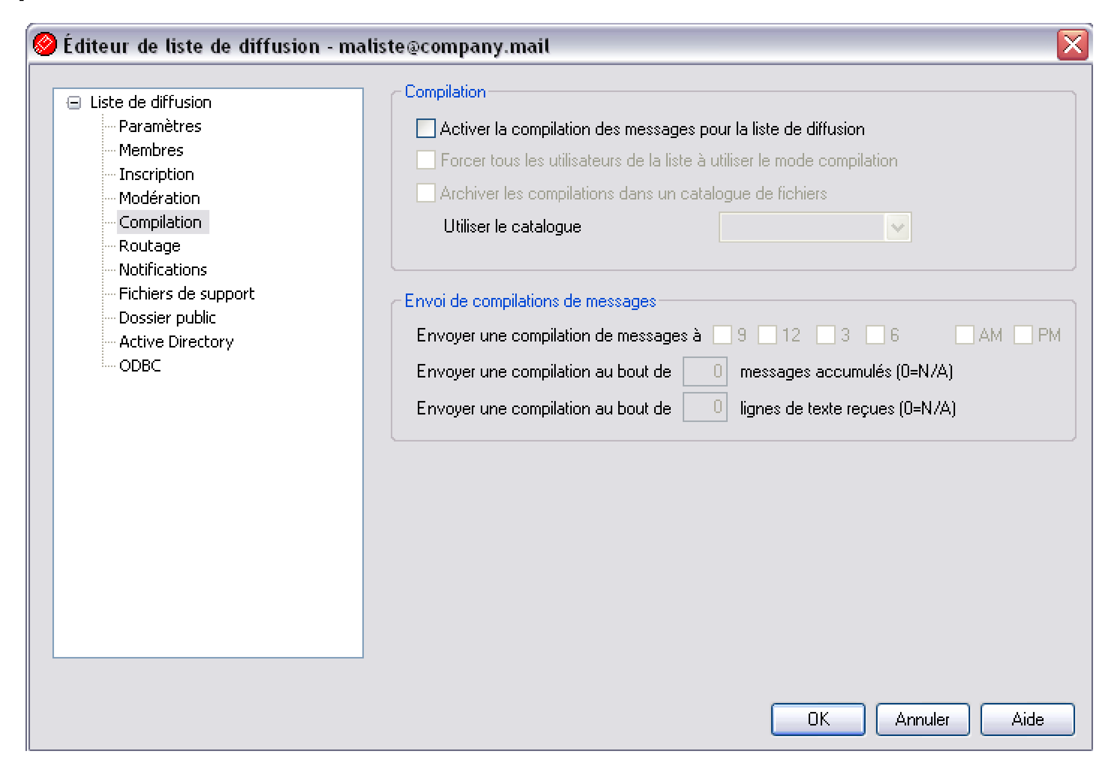
Cette liste est modérée par
Si vous sélectionnez cette option, la liste sera modérée par l'utilisateur indiqué. Les listes modérées transfèrent tous les messages au modérateur. Seul le modérateur peut soumettre ou transférer des messages à la liste.

Mot de passe
Si vous souhaitez utiliser un mot de passe, saisissez-le ici. Le mot de passe s'utilise avec l'option ci-dessus et permet également d'annuler la limite du nombre de membres indiquée dans l'onglet Inscription 384. Il donne aussi accès à diverses fonctionnalités de Contrôle du serveur à distance par e-mail 452.

Quiconque connaît le mot de passe peut poster un message
Lorsque cette option est activée, n'importe qui peut envoyer des messages à la

liste, même si elle est modérée, à condition de saisir le mot de passe au début de l'objet.

6.1.1.5 Compilation



Compilation

Activer la compilation des messages pour la liste de diffusion
Cette option détermine si la liste de diffusion prend en charge les compilations de messages. Lorsque le support de compilation est activé, une copie de chaque message envoyé à la liste de diffusion est archivée. Les membres de la liste de diffusion qui ont choisi de recevoir les messages de la liste en mode compilation recevront ces messages archivés dans un format indexé, compact et facile à utiliser.

Forcer tous les membres de la liste à utiliser le mode compilation
Par défaut, les membres de la liste peuvent choisir s'ils souhaitent recevoir les messages de la liste en mode compilation ou normal. Cette option oblige tous les membres à utiliser le mode compilation quel que soit le mode qu'ils ont choisi.

Archiver les compilations dans un catalogue de fichiers / Utiliser le catalogue :
Ces options vous permettent de placer les messages compilés dans un fichier catalogue afin que les compilations puissent être collectées plus tard. MDaemon génère un nom d'archive unique pour chaque compilation et la place dans le catalogue que vous avez indiqué.

Pour plus d’informations sur les catalogues voir : Catalogues 426.

Envoi de compilations de messages

Les compilations de liste de diffusion doivent être envoyées régulièrement aux membres de la liste qui ont choisi de recevoir les messages en mode compilation. Ces options vous permettent de définir le moment de l’envoi de la compilation par MDaemon.

Envoyer un message compilation à 9, 12, 3, 6 AM/PM
Si vous cochez toutes les cases les compilations sont envoyées toutes les 3 heures, en plus des envois déclenchés par les options ci-dessous.

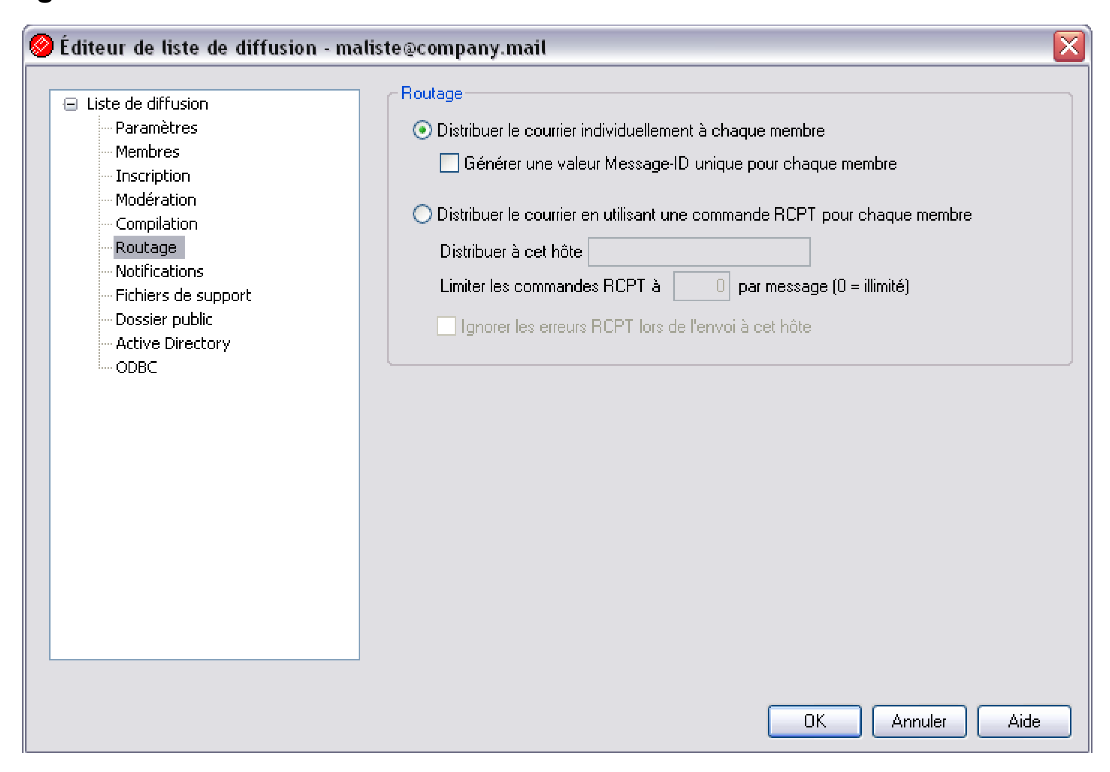
Envoyer une compilation au bout de [XX]messages accumulés (0 = N/A)
Cette option permet d’indiquer le nombre de messages que la liste accumulera avant d’envoyer les compilations aux membres de la liste en mode compilation.

Envoyer une compilation au bout de [X] lignes de texte reçues (0 = N/A)
Avec cette option, le courrier compilé est envoyé immédiatement dès qu’une compilation atteint un certain nombre de lignes de texte.

Voir également :

Membres 381
Éditeur de catalogue 426
Contrôle du serveur à distance par email 452

6.1.1.6 Routage



Routage

Distribuer le courrier individuellement à chaque membre
Si vous sélectionnez cette option, les messages de liste individuels seront crées et distribués à chaque membre de la liste. De nombreux messages individuels seront créés et cela pourrait affecter les performances du serveur.

Générer une valeur Message-ID unique pour chaque membre
Cochez cette case si vous souhaitez que chaque message possède un Message-ID unique.

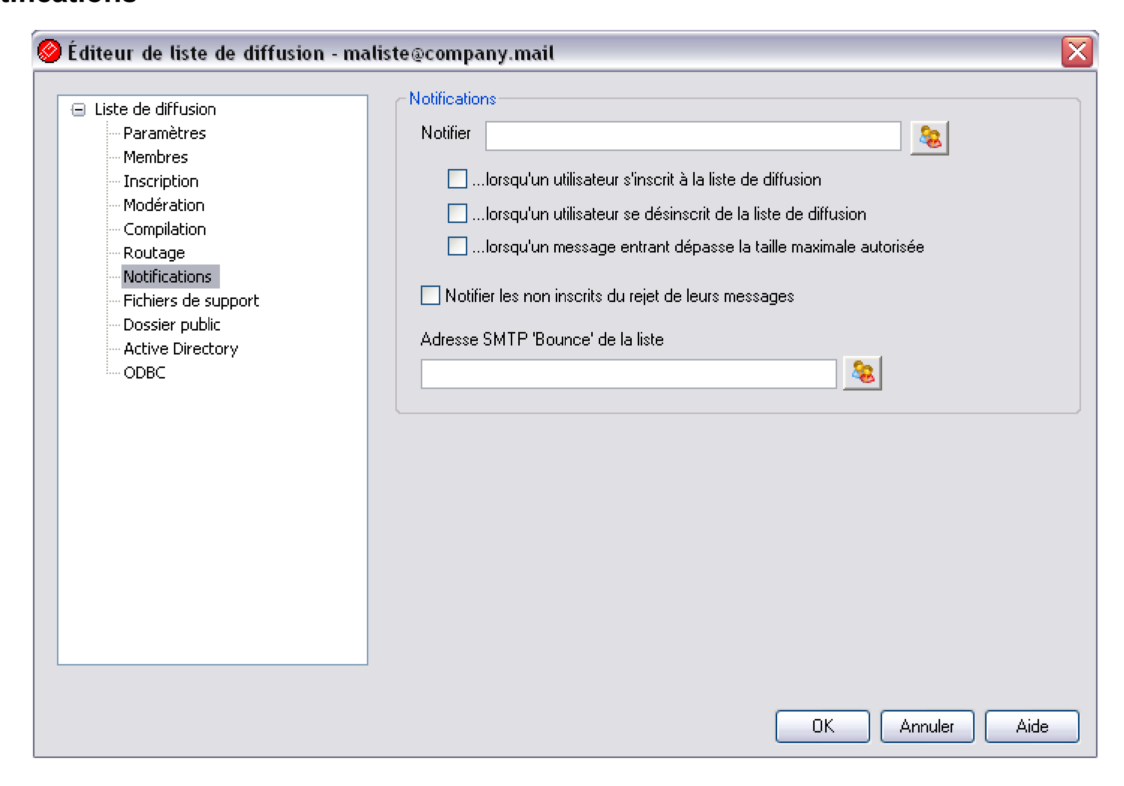
Distribuer en utilisant une commande RCPT pour chaque membre
Si vous sélectionnez cette option, MDaemon routera une seule copie de chaque message de la liste vers l'hôte de relais indiqué. Cette méthode utilise plusieurs commandes RCPT TO lors de la session SMTP avec l'hôte indiqué.

Distribuer à cet hôte
Hôte auquel les messages de la liste doivent être envoyés.

Limiter les commandes RCPT à [xx] par message (0=illimité)
Certains hôtes limitent le nombre de commandes RCPT TO qu'ils acceptent lorsque vous tentez de router une seule copie d'un message par le biais de ces hôtes. Si vous indiquez une limite dans cette commande, MDaemon la contourne en créant des copies supplémentaires du message et en divisant la liste en plus petits groupes. Ensuite, il distribue le message aux groupes en ne dépassant pas la limite.

Ignorer les erreur RCPT lors de l'envoi à cet hôte
Comme certains hôtes de relais refusent de placer en file d'attente ou de transmettre le courrier pour certains domaines, l'approche de distribution de la liste peut provoquer de nombreux problèmes. A cause d'un code erreur retourné par l'hôte relais à la suite de ce refus, MDaemon abandonne la tentative de distribution. Si ce paramètre est sélectionné, MDaemon ignorera les codes erreur retournés par l'hôte relais lors de la distribution de courrier de liste routé, permettant ainsi aux membres de recevoir le message de la liste.

6.1.1.7 Notifications



Notifications

Notifier
Indiquez l'adresse à laquelle les notifications seront envoyées.

...lorsqu'un utilisateur s'inscrit à la liste de diffusion
Si vous sélectionnez cette option, un avertissement est envoyé à l'adresse indiquée chaque fois qu'un utilisateur s'inscrit à la liste de diffusion.

...lorsqu'un utilisateur se désinscrit de la liste de diffusion
Si vous sélectionnez cette option, un avertissement est envoyé à l'adresse indiquée chaque fois qu'un utilisateur se désinscrit de la liste de diffusion.

...lorsqu'un message entrant dépasse la taille maximale autorisée
Si vous sélectionnez cette option, un avertissement est envoyé à l'adresse indiquée chaque fois qu'un utilisateur envoie à la liste de diffusion un message

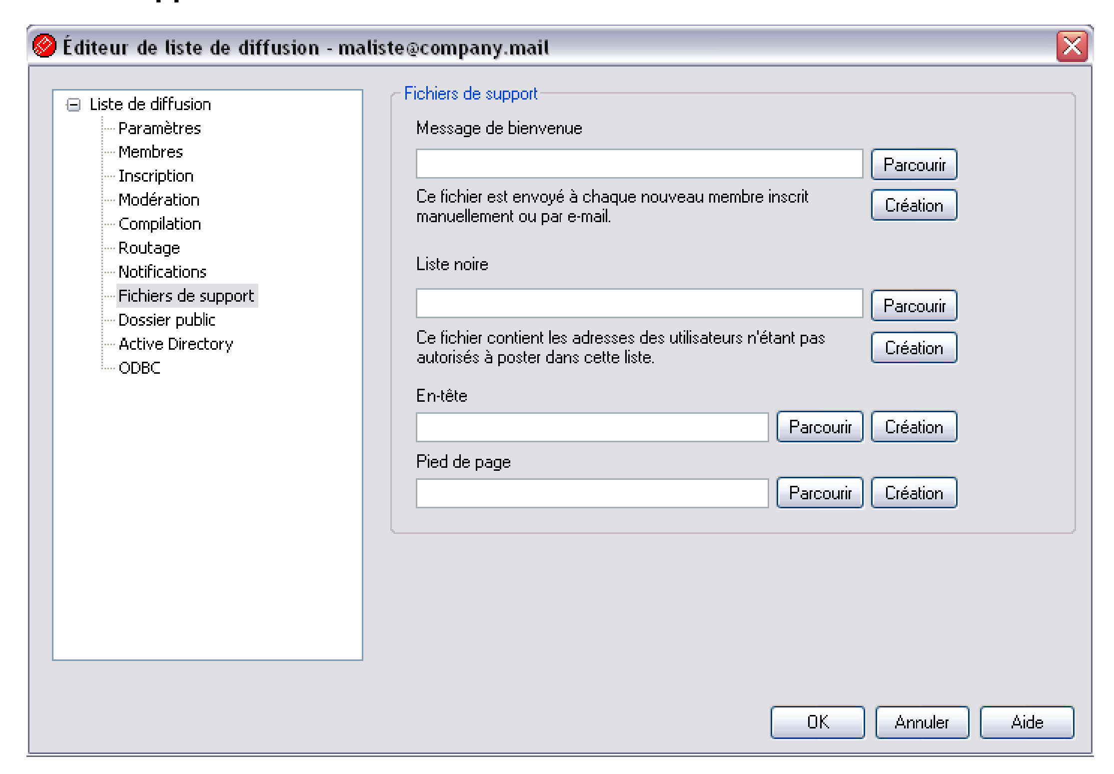
dont la taille excède la valeur maximale autorisée dans Paramètres 379.

Notifier les non inscrits du rejet de leurs messages
Lorsque des non membres d'une liste privée envoient un message à la liste, MDaemon les informe que la liste est privée. Ils reçoivent également les instructions concernant la méthode d'inscription aux listes.

Courrier renvoyé

Adresse SMTP 'Bounce' de la liste
Vous pouvez indiquer dans ce champ l'adresse qui recevra tout le courrier retourné généré par le trafic de la liste. Par exemple, une liste de diffusion comprenant 100 membres risque de contenir de 10 à 20 adresses invalides en raison de changements d'adresse, de serveurs indisponibles, etc. Le système SMTP génère et retourne alors à l'expéditeur du message un message de notification concernant l'impossibilité de distribuer le message. Si vous n'indiquez aucune adresse, MDaemon place le courrier de la liste dans le flux de messages afin qu'il ne soit pas possible de retourner du courrier.

6.1.1.8 Fichiers de support



Fichiers de support

Message de bienvenue
Si vous indiquez un fichier, il sera traité et envoyé à tous les nouveaux membres juste après leur inscription. Vous pouvez utiliser les macros suivantes :

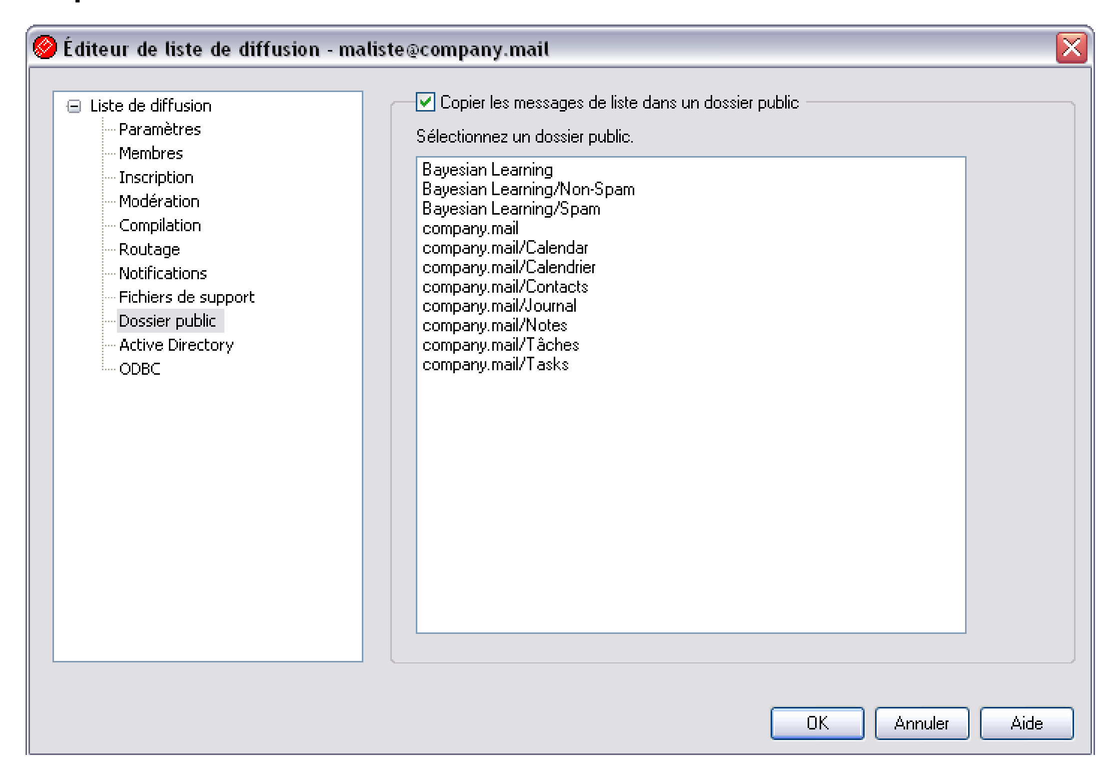
$PRIMARYDOMAIN$	Domaine par défaut de MDaemon.
$PRIMARYIP$	Adresse IP associée au domaine par défaut de MDaemon.
$MACHINENAME$	Valeur contenue dans le champ Nom de domaine complet des propriétés du domaine par défaut de MDaemon.
$LISTEMAIL$	Adresse e-mail de la liste. Exemple : maliste@exemple.com
$LISTNAME$	Nom de la liste de diffusion. Exemple : maliste
$LISTDOMAIN$	Domaine de la liste. Exemple : exemple.com
%SETSUBJECT%	Objet du message de bienvenue. Ce message peut inclure d'autres macros. Exemple : %SetSubject%=Bienvenue sur la liste $LISTNAME$.

Liste noire
Si vous avez indiqué un fichier, il sera utilisé pour supprimer les messages envoyés par les utilisateurs figurant dans la lsite.

En-tête/Pied de page
Le contenu des fichiers indiqués dans ce champ sera utilisé comme en-tête ou pied de page pour les messages de la liste.

Créer
Pour créer un nouveau fichier, cliquez sur ce bouton, choisissez un nom, puis cliquez sur *Ouvrir*. Le nouveau fichier s'ouvre alors dans le Bloc-notes.

6.1.1.9 Dossier public

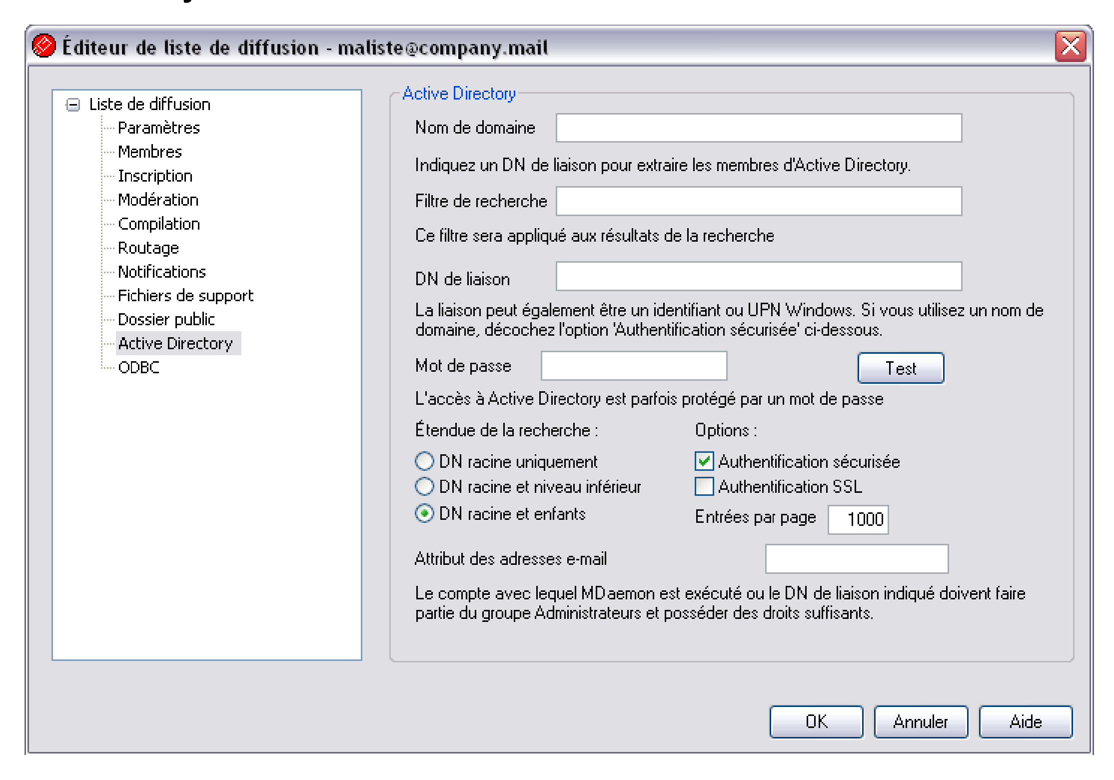


MDaemon permet l'utilisation de dossiers publics IMAP 64 avec les listes de diffusion. Les dossiers publics sont des dossiers supplémentaires disponibles pour plusieurs utilisateurs IMAP, contrairement aux dossiers IMAP personnels qui ne sont accessibles que par un utilisateur. Les options de cet onglet permettent de copier automatiquement dans un dossier public tous les messages destinés à cette liste de diffusion.

Copier les messages de liste dans un dossier public
Activez cette option si vous souhaitez que les messages de cette liste soient copiés vers un de vos dossiers publics en plus d'être distribués normalement à la liste.

Sélectionnez un dossier public
Cliquez sur le dossier public que vous souhaitez associer aux messages de cette liste.

6.1.1.10 Active Directory



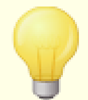
Cet onglet permet d'extraire d'Active Directory les adresses des membres de la liste.

Active Directory

Nom de domaine
DN racine de l'arborescence, dans lequel MDaemon recherche les comptes. Par défaut, il recherche "Root DSE", qui correspond au point le plus haut dans la hiérarchie de Active Directory. Vous pouvez réduire la durée de la recherche en désignant un point de départ plus près de l'emplacement des comptes dans votre arborescence. Si vous ne remplissez pas ce champ, MDaemon utilise la valeur par défaut : `LDAP://rootDSE`

Filtre de recherche
Filtre de recherche LDAP appliqué lors de la vérification des comptes dans Active Directory. Il permet de déterminer de façon plus précise les comptes que vous souhaitez inclure.

DN de liaison
DN utilisé par MDaemon pour effectuer la liaison avec Active Directory. Vous pouvez indiquer un compte Windows ou un chemin UPN.



Si vous utilisez un DN au lieu d'un identifiant Windows, vous devez désactiver l'option *Authentification sécurisée* ci-dessous.

Mot de passe
Mot de passe correspondant au DN ou à l'identifiant Windows défini dans l'option précédente.

Test
Cliquez sur ce bouton pour tester la configuration des paramètres Active Directory de MDaemon.

Étendue de la recherche :

DN racine uniquement
Limite la recherche au DN indiqué ci-dessus.

DN racine et niveau inférieur
Étend la recherche au niveau situé au-dessous du DN racine dans l'arborescence.

DN racine et enfants
Étend la recherche à tous les enfants du DN racine, jusqu'au niveau le plus bas. Cette option est appliquée par défaut.

Options :

Authentification sécurisée
Cochez cette option si vous souhaitez utiliser une authentification sécurisée lors des recherches dans Active Directory. Vous ne pouvez pas l'utiliser si vous avez choisi un DN et non un identifiant Windows pour le champ *DN de liaison*.

Authentification SSL
Cochez cette option si vous souhaitez utiliser une authentification SSL lors des recherches dans Active Directory.



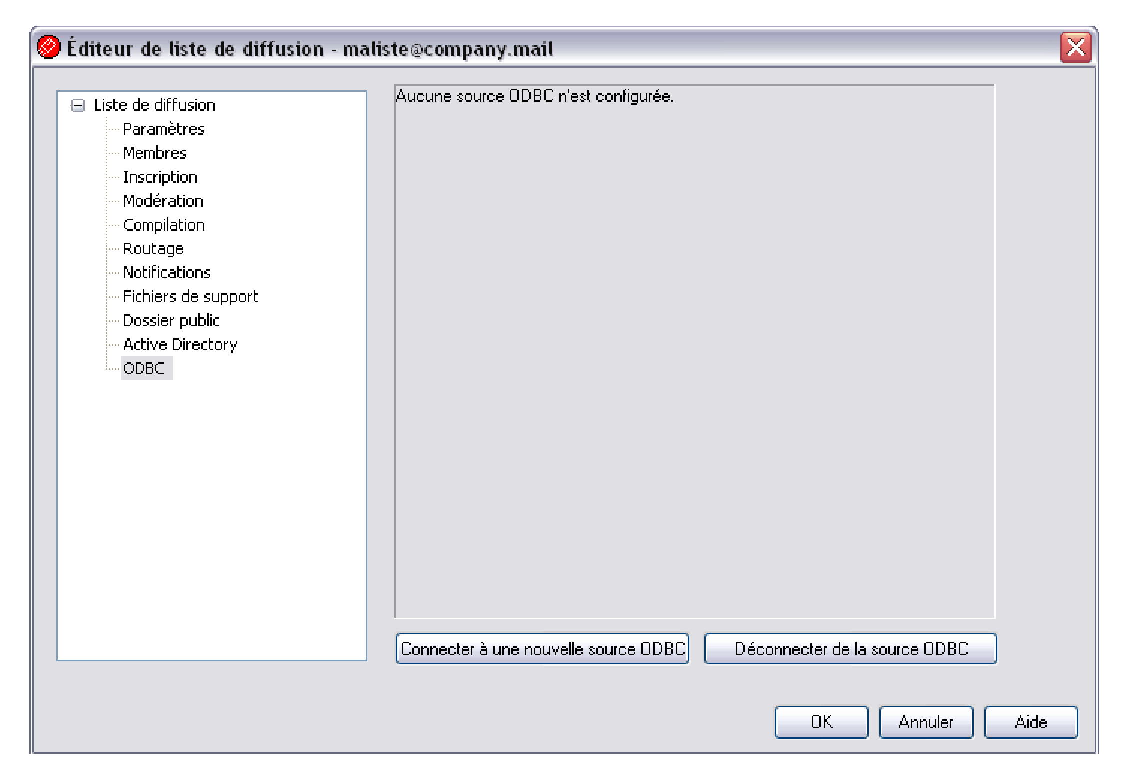
Cette option requiert un serveur et une infrastructure SSL dans votre réseau Windows et Active Directory. En cas de doute, contactez votre administrateur réseau.

Entrées par page
Si les résultats d'une requête Active Directory sont supérieurs au nombre d'entrées indiquées, ils seront inclus dans plusieurs pages. Indiquez ici le nombre maximum d'entrées par page.

Attribut des adresses e-mail

Indiquez dans ce champ l'attribut contenant les adresses e-mail. Par exemple, si vous indiquez "Mail", chaque compte Active Directory que vous souhaitez intégrer à la liste doit posséder un attribut "Mail" contenant son adresse.

6.1.1.11 ODBC



Avec cette fonctionnalité, vous pouvez effectuer la maintenance des membres de vos listes de diffusion dans une base de données compatible ODBC. Cet onglet sert à sélectionner une source de données, une liste et des mappages de champs que MDaemon lie à la liste. Lorsque des messages arrivent pour votre liste, une ou plusieurs requêtes SQL sont effectuées automatiquement et les adresses électroniques en résultant sont traitées comme des membres de la liste.

Vous pouvez ajouter, retirer et modifier des membres de votre liste dans la base de données à l'aide de l'application de base de données compatible ODBC de votre choix.

ODBC

Dans cette section s'affichent les propriétés actuelles ODBC que vous avez configurées pour la liste de diffusion. Les mappages de champs de la base de données et les requêtes SQL que vous avez configurées pour indiquer le statut de chaque membre s'affichent ici (Normal, Envoi seul, Lecture seule, et/ou Mode compilation).

Connecter à une nouvelle source ODBC

Cliquez sur ce bouton pour ouvrir l'Assistant de sélection ODBC afin de choisir la source de base de données système que vous souhaitez utiliser pour la liste de diffusion.

Déconnecter de la source ODBC

Cliquez sur ce bouton pour dissocier la liste de la source de données ODBC.

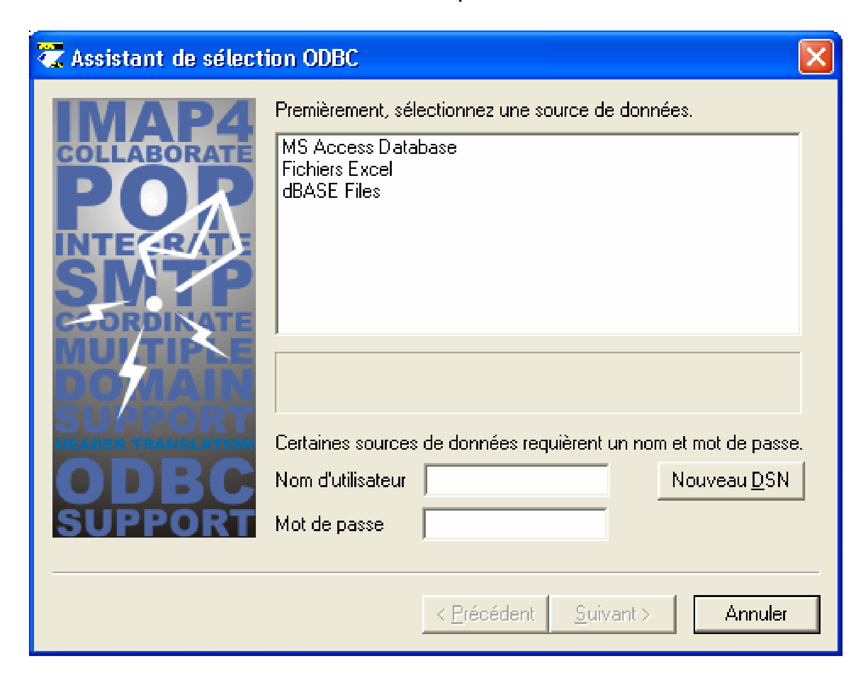
Voir également :

Configuration d'une source de données ODBC pour une liste de diffusion 398
Création d'une nouvelle source de données ODBC 400

6.1.1.11.1 Configuration d'une source de données ODBC pour une liste de diffusion

Pour utiliser une base de données accessible via ODBC, avec une liste de diffusion :

1. Cliquez sur *Connecter à une nouvelle source ODBC* dans l'onglet ODBC 397 de l'Éditeur de liste de diffusion pour ouvrir l'Assistant de sélection ODBC.



2. Sélectionnez la source de données que vous souhaitez utiliser pour la liste de diffusion. Si aucune source de données système compatible n'est répertoriée, créez-en une nouvelle en suivant les instructions fournies dans **Création d'une nouvelle source de données ODBC** 362.

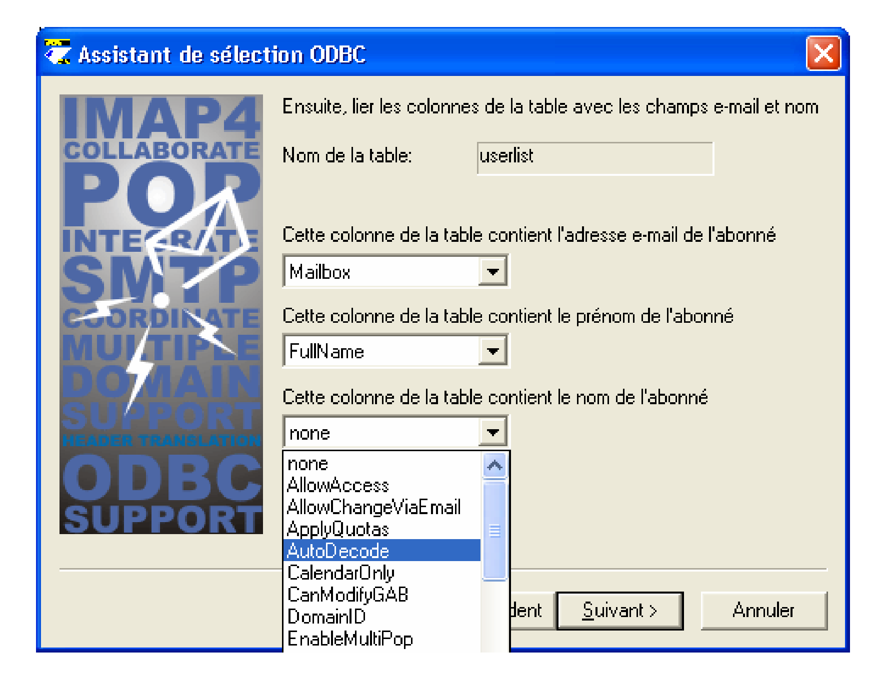
3. Si nécessaire, indiquez un identifiant et un mot de passe.

4. Cliquez sur Suivant.

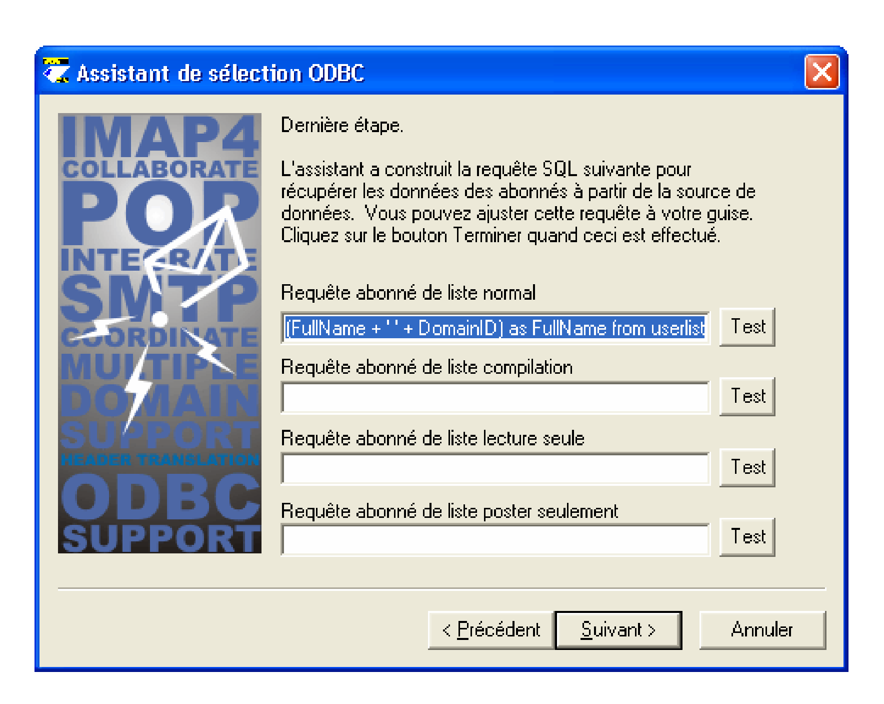
5. La source de données doit contenir au moins une table avec des champs pour l'adresse électronique et le nom. Si la source de données contient au moins une table qualifiée, choisissez la table voulue, puis cliquez sur *Suivant*. Sinon, cliquez sur *Annuler* pour sortir de l'Assistant de sélection ODBC et utilisez votre application de base de données pour ajouter une table dans la base de données adéquate avant de continuer.



6. Sélectionnez dans le menu déroulant les champs de la table qui correspondent à l'adresse électronique, au prénom et au nom. Cliquez sur *Suivant*.



7. L'Assistant de sélection ODBC élabore une requête SQL en fonction des éléments que vous avez sélectionnés à l'étape 6. MDaemon l'utilise pour extraire les données des membres de la liste de votre base de données. Vous pouvez les modifier comme vous le souhaitez et inclure d'autres requêtes dans les commandes pour que les membres reçoivent les messages en mode Compilation et pour indiquer des membres en lecture ou en envoi seuls. Un bouton *Test* se trouve à côté de chaque commande et permet de tester vos requêtes afin de vous assurer qu'elles extraient les données adéquates.



8. Cliquez sur *Terminer*.

Voir également :

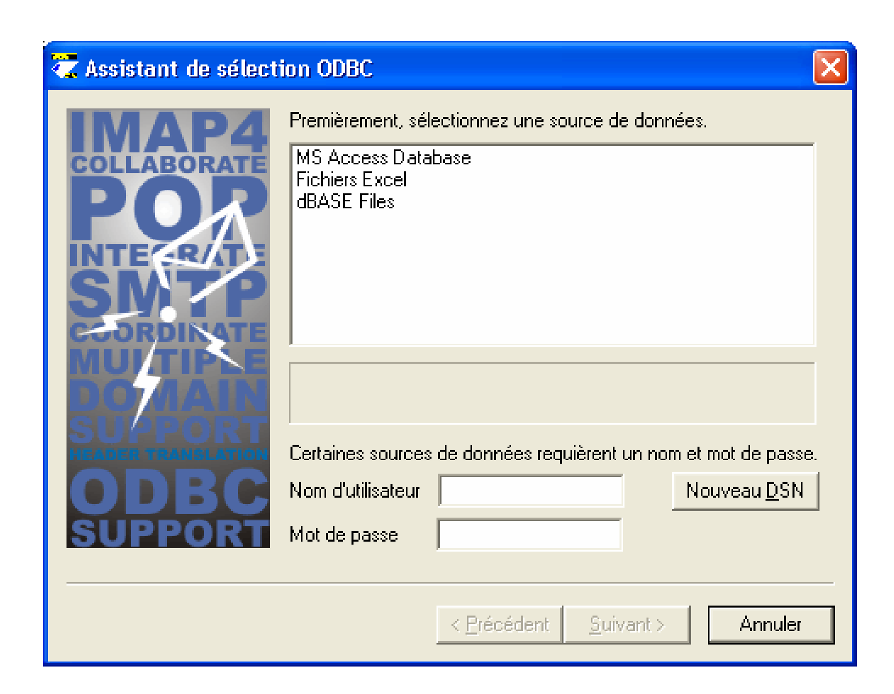
Éditeur de liste diffusion » ODBC 397
Création d'une source de données ODBC 400

6.1.1.11.2 Création d'une nouvelle source de données ODBC

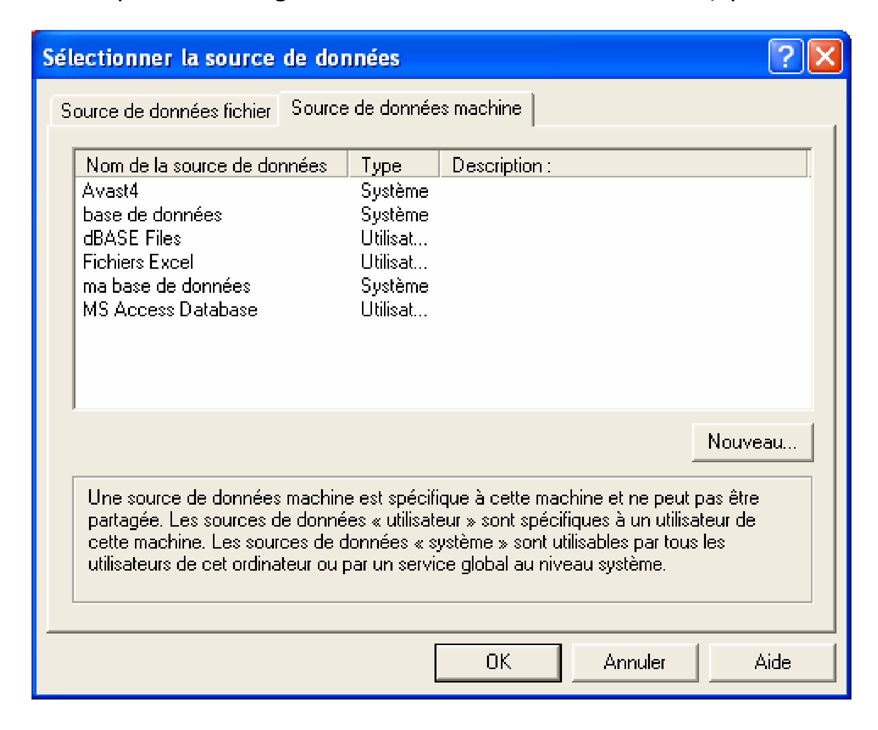
Pour créer une nouvelle source de données ODBC :

1. Cliquez sur *Connecter à une nouvelle source ODBC* dans l'onglet ODBC 397 de l'Éditeur de liste de diffusion pour ouvrir l'Assistant de sélection ODBC.

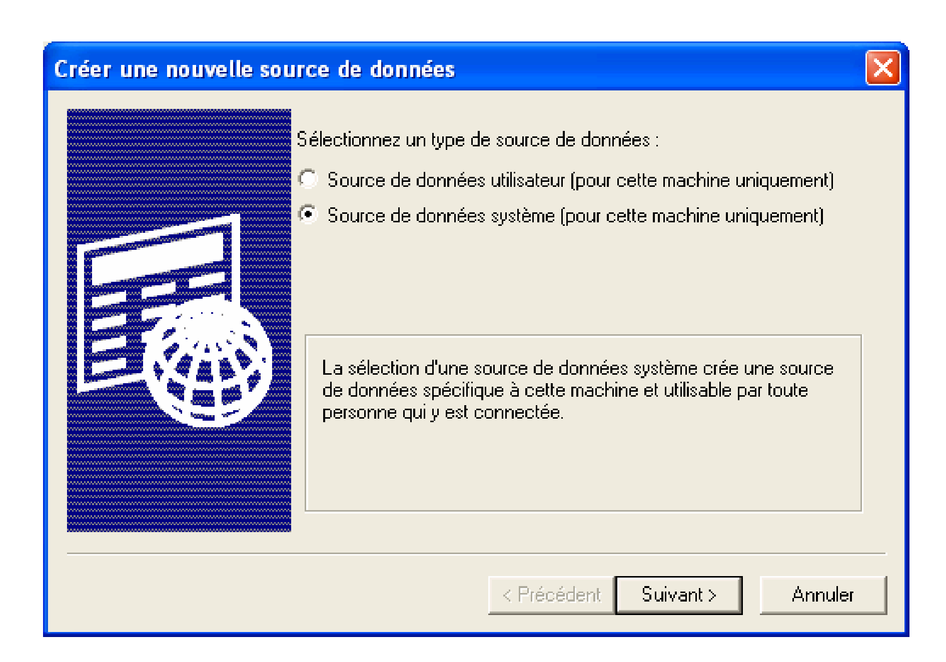
2. Cliquez sur *Nouveau DSN* pour ouvrir la boîte de dialogue *Sélectionner la source de données*.



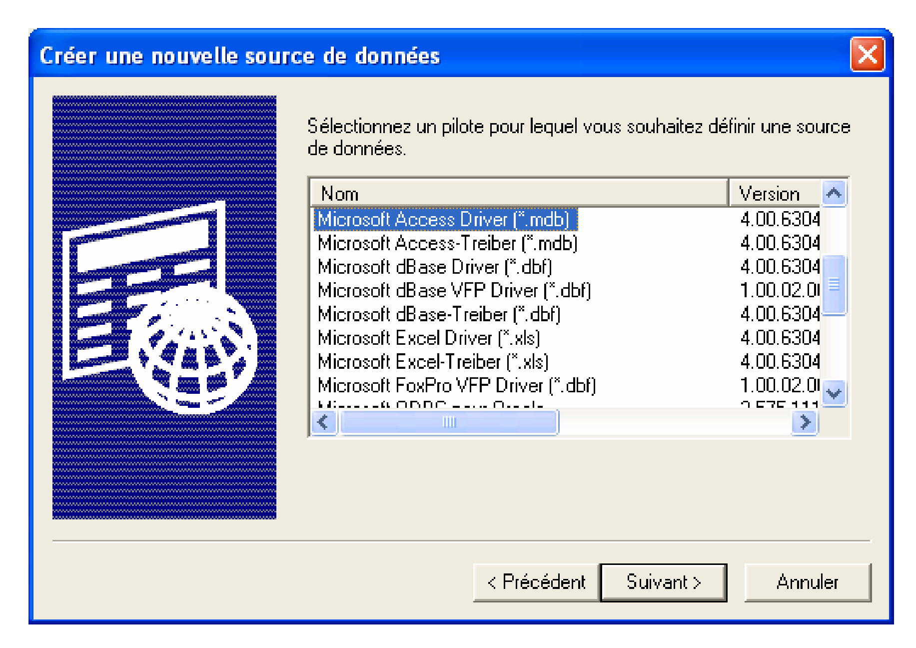
3. Cliquez sur l'onglet *Source de données machine*, puis sur *Nouveau...*.



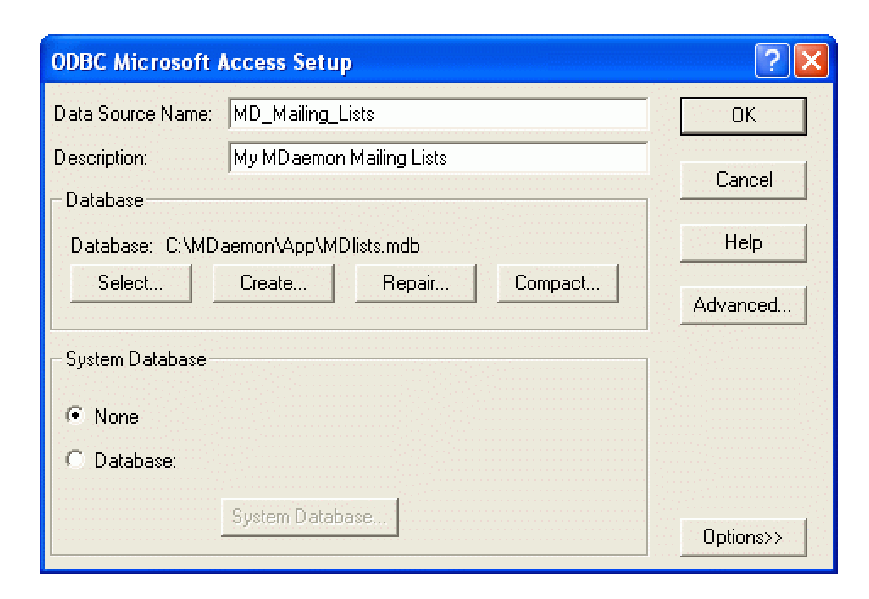
4. Sélectionnez *Source de données système*, puis cliquez sur Suivant.



5. Sélectionnez le pilote de base de données pour lequel vous souhaitez définir une source de données, puis cliquez sur *Suivant*.



6. Cliquez sur *Terminer* pour afficher la boîte de dialogue de configuration du pilote. Cette boîte de dialogue dépendra du pilote que vous avez sélectionné (ici : boîte de dialogue de configuration de Microsoft Access).



7. Indiquez un nom pour votre nouvelle source de données et fournissez les informations requises dans la boîte de dialogue du pilote (comme créer ou indiquer une base de données, choisir un répertoire ou un serveur, etc.).

8. Cliquez sur *OK* pour fermer la boîte de dialogue du pilote.

9. Cliquez sur *OK* pour fermer la boîte de dialogue *Base de données des comptes*.

Voir également :

ODBC - Liste de diffusion 397
Configuration d'une source de données ODBC pour une liste de diffusion 398



Section VII

7 Menu Passerelles

7.1 Passerelles de domaine

L'Éditeur de passerelle 407 est un outil de MDaemon PRO. Pour y accéder, cliquez sur Passerelles » Nouvelle passerelle ou Passerelles » Modifier une passerelle. Cette fonctionnalité permet de prendre en charge de façon limitée mais efficace l'hebergement de plusieurs domaines ou de fonctionner en tant que serveur secondaire.

Par exemple :

> Vous souhaitez servir de serveur secondaire pour une organisation tierce, recevoir son courrier entrant et le stocker sur un dossier de votre serveur. Par contre, vous ne voulez pas héberger complètement son domaine, ni assurer la maintenance des comptes. Le nom de domaine de cette organisation est "`company.com`".
>
> Tout d'abord, saisissez "`company.com`" dans le champ *Nom de domaine* de l'onglet Domaine. Indiquez ensuitre le dossier dans lequel les messages de ce domaine seront stockés. Tous les messages reçus pour ce domaine seront extraits du flux de courrier et placés dans ce dossier, quel que soit le destinatiare.
>
> Ensuite, choisissez les méthodes de collecte ou de distribution à utiliser pour que le courrier soit envoyé sur le serveur de ce domaine, sur lequel les comptes sont hébergés. Pour cela, vous disposez de trois possibilités : *Distribuer les messages enregistrés à chaque traitement du courrier distant* (dans l'onglet Domaine 408, les options de Retrait de la file d'attente 414, ou la configuration d'un compte 416 spécifique pour ce domaine).
>
> Enfin, vous devrez probablement modifier les DNS du domaine `company.com` afin que votre serveur MDaemon y figure en tant qu'hôte MX autorisé.

L'exemple ci-dessus illustre une des utilisations les plus courantes, mais les passerelles offrent de nombreuses fonctionnalités supplémentaires. En effet, certaines situations particulières, comme l'utilisation d'un nom de domaine qui n'existe pas, nécessitent une configuration spécifique. Il est possible de recevoir des messages pour un domaine non enregistré, mais dans ce cas le nom du domaine doit être "masqué" dans une adresse du Domaine par défaut 33. Par exemple, si votre domaine par défaut est `exemple.com` et que vous avez créé une passerelle pour `company.mail`, il est possible d'envoyer un message à "`bob@company.mail`" en utilisant l'adresse "`bob{company.mail}@exemple.com`". Lorsque MDaemon reçoit un tel message, il convertit l'adresse en "`bob@company.mail`" et distribue le message dans le dossier attribué à la passerelle. Il est évidemment plus simple d'enregistrer un nom de domaine valide pour la passerelle.

Voir également :

Éditeur de passerelle 407
Domaine par défaut 33
Domaines supplémentaires 103

7.1.1 Éditeur de passerelles

L'Éditeur de passerelles s'affiche en cliquant sur Passerelles » Nouvelle passerelle... ou sur Passerelles » Modifier une passerelle... Il contient les onglets suivants :

Domaine 408
Cette boîte de dialogue contient le nom de domaine du domaine avec lequel vous travaillez, ainsi que le chemin vers le répertoire utilisé pour stocker les messages pour ce domaine.

Vérification 409
Si le serveur du domaine distant possède une base de données des utilisateurs, alias et listes de diffusion (LDAP ou Active Directory), ou un serveur Minger pour la vérification des adresses ; il est possible de vérifier la validité des destinataires des messages entrants. Si l'adresse du destinataire est invalide, le message est rejeté. Cette méthode évite de devoir accepter tous les messages sans vérifier l'adresse du destinataire.

Transfert 413
Vous pouvez indiquer un hôte auquel le courrier du domaine sera transféré dès son arrivée. Il existe également des options permettant de préciser si une copie de ces messages sera ou non conservée localement, ainsi que le numéro de port sur lequel sont transférés les messages.

Retrait de la file d'attente 414
Utilisez les commandes de cette boîte de dialogue pour choisir si MDaemon répondra ou non aux requêtes ETRN ou ATRN effectuées pour le compte du domaine afin de sortir ses messages de la file d'attente.

Compte 416
Vous pouvez créer ici un compte POP ou IMAP qui aura accès au courrier stocké de ce domaine. Á l'aide du nom et du mot de passe qui sont indiqués ici, un client de messagerie ordinaire ou une autre installation MDaemon peuvent avoir accès à la boîte aux lettres du domaine et collecter son courrier.

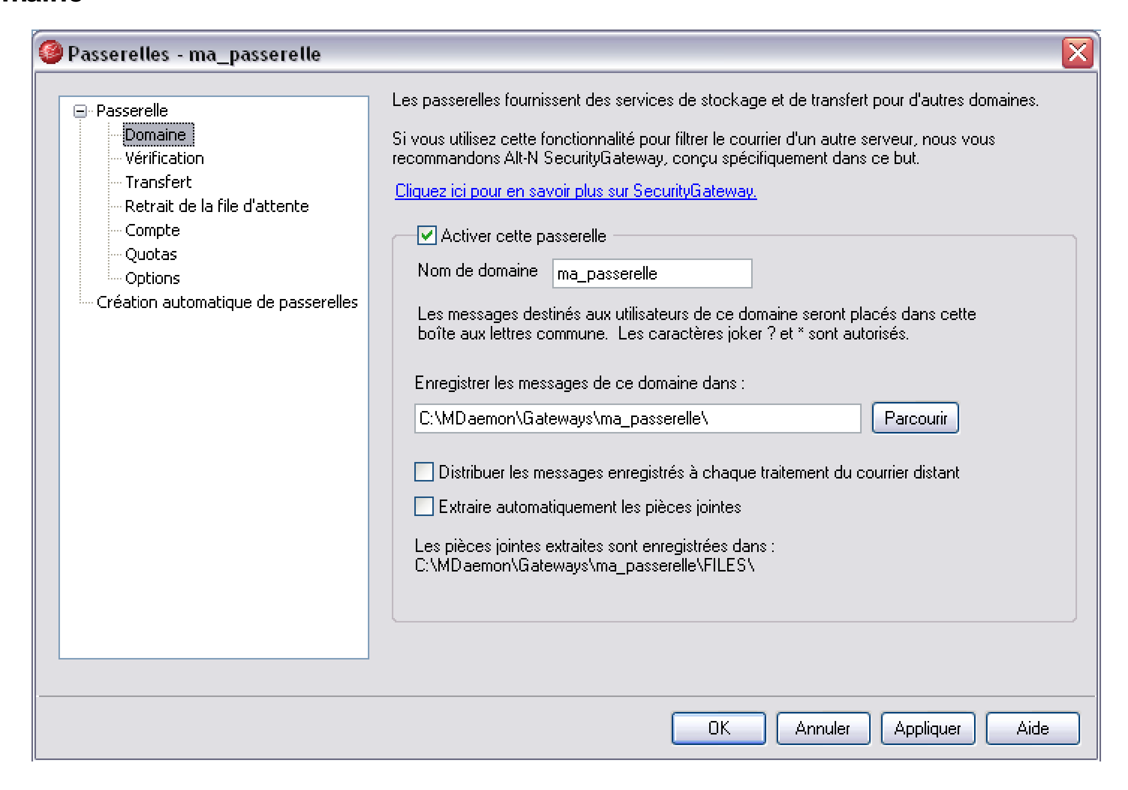
Quotas 417
Cette boîte de dialogue sert à indiquer une limite du total de l'espace disque que le domaine peut utiliser et le nombre maximum de messages qui peuvent être stockés.

Options 418
Cet onglet contient diverses options appliquées à la passerelle sélectionnée.

Voir également :

Passerelles de domaine 406

7.1.1.1 Domaine



Activer cette passerelle
Cochez cette case pour que MDaemon collecte le courrier de la passerelle. Si vous la décochez, MDaemon ne collecte plus les messages pour cette passerelle, mais ses paramètres sont conservés.

Nom de domaine
Entrez le nom du domaine pour lequel vous souhaitez que MDaemon agisse en tant que passerelle de messagerie.

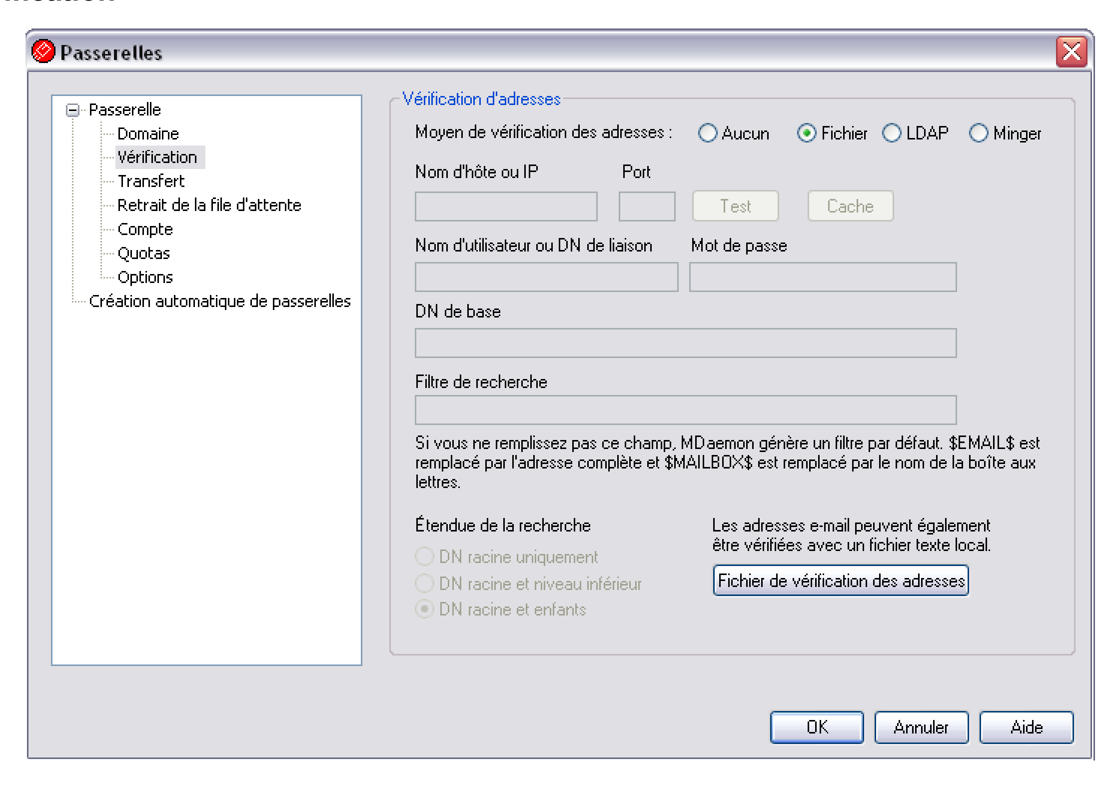
Enregistrer les messages de ce domaine dans :
Indiquez le répertoire dans lequel vous voulez que le courrier entrant pour le domaine soit stocké. Tout le courrier entrant destiné à ce domaine sera stocké dans ce répertoire, quel que soit le destinataire.

Distribuer les messages enregistrés à chaque traitement du courrier distant
D'ordinaire, lorsque MDaemon reçoit du courrier destiné à une de ses passerelles de domaine, il stocke ses messages jusqu'à ce que ce domaine se connecte à MDaemon pour le collecter. Dans certains cas, vous pouvez souhaiter que MDaemon tente de distribuer le courrier directement via SMTP plutôt que d'attendre que le domaine ne le collecte. Lorsque cette option est activée, MDaemon tente de distribuer les messages de ce domaine à chaque intervalle de traitement du courrier distant. La boîte aux lettres de la passerelle agira temporairement comme une file d'attente distante et le courrier tentera d'être distribué. Les messages ne pouvant pas être distribués resteront simplement dans la boîte aux lettres de la passerelle jusqu'à ce qu'ils soient collectés par le domaine ou distribués plus tard avec succès, ils ne seront pas déplacés vers la file d'attente distante ou le système de relance.

Cependant, si les DNS du domaine ne sont pas configurés correctement, ou si votre serveur MDaemon est configuré pour envoyer tous les messages sortants à un hôte de relais, ces messages risquent de causer une boucle de courrier et d'être considérés comme non distribuables.

Extraire automatiquement les pièces jointes
Certains systèmes de messagerie nécessitent que les pièces jointes soient extraites avant que les messages ne soient soumis au flux de courrier. Pour faciliter cela, MDaemon peut extraire automatiquement les pièces jointes MIME entrantes et les placer dans un sous-dossier \Files\ du répertoire de messages du domaine. Ce sous-dossier ne sera utilisé que si cette option est activée.

7.1.1.2 Vérification



Souvent, les passerelles de domaine ne possèdent pas de système permettant de déterminer si le destinataire d'un message entrant est valide ou non. Par exemple, si un message destiné à frank@exemple.com arrive sur le serveur de passerelle exemple.com, ce dernier n'a aucun moyen de savoir s'il existe une boîte aux lettres, un alias ou une liste de diffusion pour "frank" sur exemple.com. Ainsi, le serveur de passerelle est obligé d'accepter tout le courrier. Cela peut poser des problèmes de spam, car les spammeurs envoient généralement leurs messages à un grand nombre d'adresses invalides.

Pour résoudre ce problème, MDaemon contient un système qui permet de vérifier les adresses dans les messages entrants. Si le serveur distant possède un serveur Minger pour la vérification des comptes ou une base de données LDAP ou Active Directory

contenant les boîtes aux lettres, alias et listes de diffusion, cet onglet permet de les utiliser pour vérifier les adresses.

Vérification d'adresses

Moyen de vérification des adresses :

Aucun
Sélectionnez cette option si vous ne souhaitez pas vérifier les adresses des destinataires des messages pour cette passerelle. MDaemon considère alors que tous les destinataires des messages entrants sont valides.

Fichier
Sélectionnez cette option pour choisir comme moyen de vérification la liste d'adresses contenues dans le fichier `GatewayUsers.dat`. Cette liste est globale pour toutes les passerelles, et peut être utilisée comme source de données supplémentaire si vous avez choisi un autre moyen de vérification. Cependant, lorsque cette option est sélectionnée, ce fichier est le seul outil de vérification des adresses. Pour modifier son contenu ou ajouter des adresses, cliquez sur le bouton *Fichier de vérification des adresses*.

LDAP
Sélectionnez cette option pour vérifier les adresses à l'aide d'un serveur LDAP ou Active Directory. À chaque réception d'un message destiné au domaine distant, une requête est envoyée au serveur LDAP ou Active Directory afin de déterminer si le destinataire est valide ou non. Si ce n'est pas le cas, le message sera rejeté. Si MDaemon ne peut pas se connecter au serveur LDAP/AD, l'adresse est considérée comme valide.

Minger
Sélectionnez cette option pour vérifier les adresses à l'aide du serveur Minger du domaine distant. Si MDaemon ne peut pas se connecter au serveur, l'adresse est considérée comme valide. L'onglet Options 418 contient également une option globale permettant d'interroger également vos hôtes de Partage de domaine 57.

Nom d'hôte ou IP
Saisissez le nom d'hôte ou l'adresse IP du serveur LDAP/Active Directory ou Minger du domaine. MDaemon se connecte à ce serveur pour vérifier la validité des adresses des destinataires lorsqu'il reçoit des messages destinés à cette passerelle.

Port
Indiquez le numéro de port utilisé par le serveur LDAP/AD/Minger du domaine.

Test
Cliquez sur ce bouton pour vérifier que les paramètres de vérification des adresses à distance sont configurés correctement. MDaemon se connecte alors au serveur LDAP/AD indiqué, et vérifie s'il reconnaît les informations saisies dans les différents champs.

Cache
Cliquez sur ce bouton pour ouvrir le fichier de cache LDAP/Minger. Le cache

s’active/se désactive dans l’onglet Options 418.

Nom d’utilisateur ou DN de liaison
Saisissez le nom d’utilisateur ou DN du compte qui possède un accès administrateur au serveur LDAP/Active Directory du domaine, pour que MDaemon puisse vérifier les adresses de la passerelle. Ce DN sert à l’authentification au cours de l’opération de liaison.

Mot de passe
Ce mot de passe, en association avec la valeur liaison DN, sera communiqué au serveur LDAP/Active Directory du domaine pour l’authentification. Si vous avez sélectionné la méthode Minger, indiquez le mot de passe pour l’authentification sur le serveur Minger.

DN de base
DN (distinguished name) ou point de départ du DIT (Directory Information Tree) sur lequel MDaemon va envoyer les requêtes pour la vérification des adresses.

Filtre de recherche
Filtre de recherche LDAP/AD utilisé lors de l’envoi de requêtes pour la vérification des adresses. MDaemon propose un filtre par défaut qui devrait fonctionner dans la plupart des cas.

Étendue de la recherche :

Étendue des vérification LDAP/AD.

DN racine uniquement
Limite la recherche au DN de base indiqué ci-dessus. La recherche ne dépasse pas ce point de l’arborescence (DIT).

DN racine et niveau inférieur
Étend la recherche au niveau inférieur au DN de base indiqué ci-dessus.

DN racine et enfants
Étend la recherche à tous les niveaux inférieurs du DN de base.

Fichier de vérification des adresses
Cliquez sur ce bouton pour ouvrir le fichier de vérification des adresses (`GatewayUsers.dat`).

Utiliser plusieurs configurations pour les requêtes LDAP

Vous pouvez utiliser plusieurs configurations LDAP pour vos passerelles de domaines. Pour utiliser une nouvelle configuration LDAP, définissez une première configuration normale puis modifiez le fichier `GATEWAYS.DAT` dans un éditeur de texte.

Les paramètres doivent être au format suivant :

```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
```

```
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

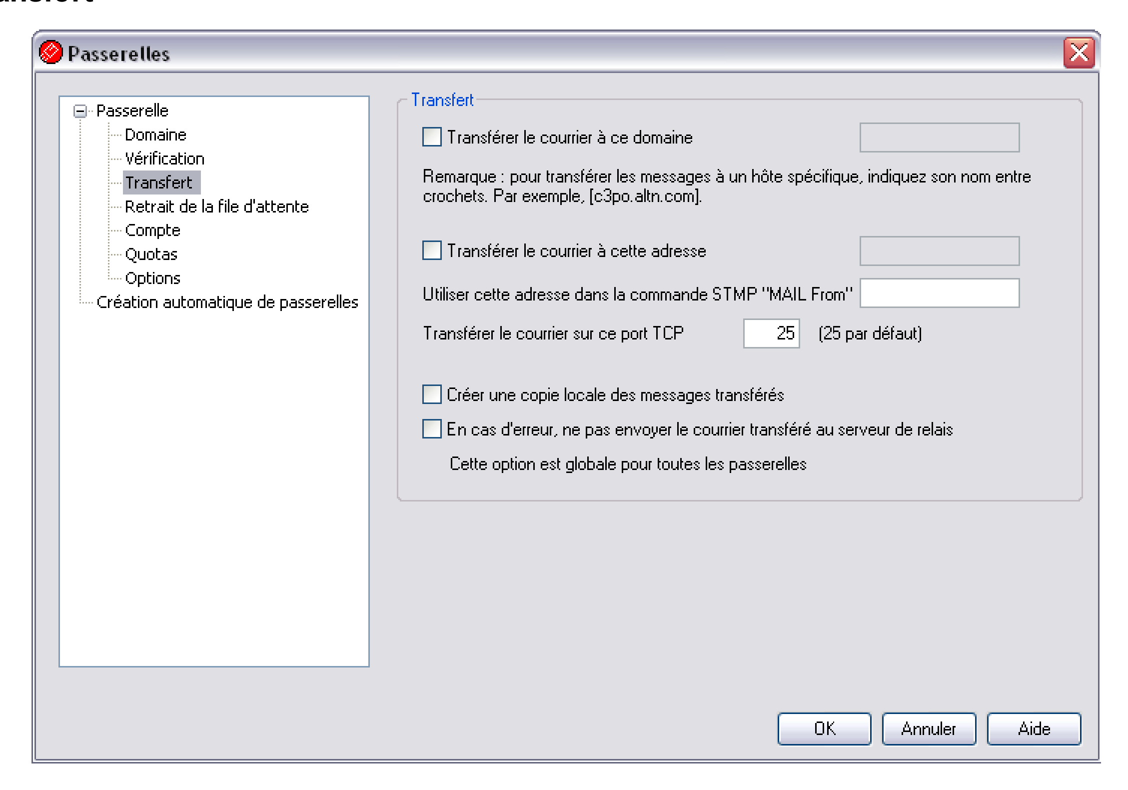
Pour chaque nouvel ensemble de paramètres, ajoutez 1 au chiffre qui se trouve à la fin de chaque ligne. Dans l'exemple donné, chaque ligne se termine par "1". Pour créer un autre ensemble de clés, terminez chaque valeur par le chiffre "2", puis "3", etc.

Lors d'une requête LDAP, MDaemon contrôle tour à tour chaque configuration pour trouver une correspondance. Si une erreur se produit ou si la correspondance est trouvée dans un ensemble, MDaemon arrête la recherche.

Voir également :

LDAP/Carnet d'adresses 89
Minger 369

7.1.1.3 Transfert



Transfert

Transférer le courrier à ce domaine
Il est parfois utile de transférer une copie de tous les messages reçus d'un domaine. Pour cela, indiquez le nom ou l'adresse IP du domaine vers lequel vous souhaitez transférer le courrier du domaine. Si vous souhaitez transférer les messages vers un hôte spécifique, indiquez son nom entre crochets (par ex. : [hote1.exemple.net]).

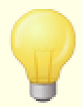
Transférer le courrier à cette adresse
Cette option transfère le courrier destiné au domaine à une adresse spécifique.

Utiliser cette adresse dans la commande SMTP "Mail From"
Adresse incluse dans la commande SMTP "Mail From".

Transférer le courrier sur ce port TCP
Port utilisé par MDaemon pour transférer le courrier.

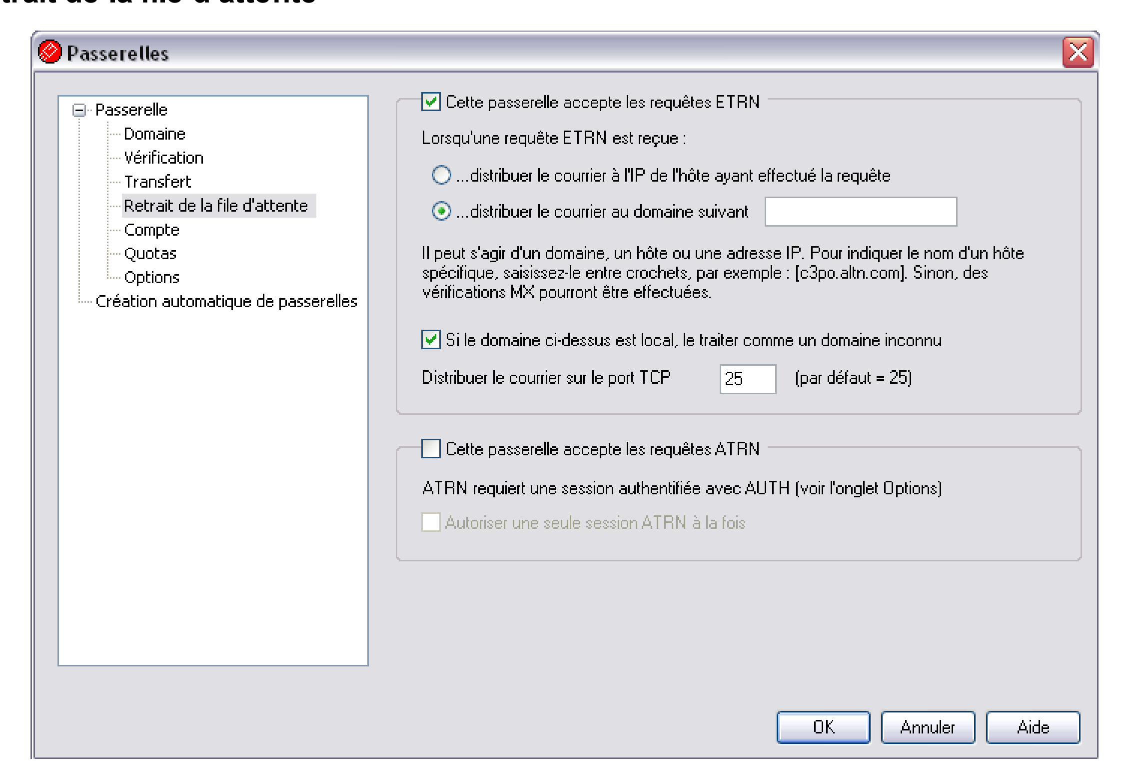
Créer une copie locale des messages transférés
Sélectionnez cette option pour conserver une copie en local des messages une fois qu'ils ont été transférés.

En cas d'erreur, ne pas envoyer le courrier transféré au serveur de relais
Cochez cette option pour ne pas envoyer ces messages au serveur de relais en cas d'erreur.



Cette option est globale et s’applique à toutes les passerelles. Elle est désactivée par défaut.

7.1.1.4 Retrait de la file d'attente



ETRN

Cette passerelle accepte les requêtes ETRN
Lorsque ce paramètre est activé, MDaemon répond aux requêtes ETRN effectuées par des hôtes qualifiés pour le compte du domaine pour lequel MDaemon agit comme passerelle de messagerie. La commande ETRN est une extension SMTP qui signale à un serveur stockant le courrier pour un compte particulier qu’il est temps de traiter le courrier. Lorsque MDaemon reçoit une requête ETRN pour un domaine, il commence immédiatement le traitement du courrier stocké qui doit être distribué à l’aide des transactions SMTP appropriées. La session SMTP qui émet une requête ETRN ne sera pas celle qui reçoit le courrier stocké. MDaemon utilisera les transactions SMTP indépendantes appropriées pour envoyer le courrier qu’il a stocké pour le domaine. Cela permet de préserver l’enveloppe du message et est plus sécurisant. De plus, l’hôte auquel MDaemon envoie le courrier stocké peut ne pas commencer immédiatement la réception de ces messages. ETRN ne fait que garantir que le courrier stocké est traité pour être distribué. Le traitement réel de la distribution est sujet aux autres restrictions imposées par l’administrateur et est susceptible de devoir attendre dans la file d’attente de courrier sortant que le prochain intervalle de traitement du courrier distant programmée ait lieu. En raison

de ces limitations, il est recommandé d'utiliser On-Demand Mail Relay (ODMR) 51 et sa commande ATRN plutôt que ETRN. Cette méthode n'est cependant pas prise en charge par tous les clients et les serveurs et n'est donc disponible que pour les domaines clients qui utilisent un serveur le permettant. MDaemon prend totalement en charge ODMR à la fois du côté client et du côté serveur.



Par défaut, MDaemon exige que l'hôte envoyant la requête ETRN utilise une session authentifiée à l'aide du *Nom de domaine* 408 et du *Mot de passe AUTH* 418 de la passerelle. Si vous souhaitez autoriser les connexions non authentifiées, décochez *Exiger une authentification pour les requêtes ETRN...* dans l'onglet Options 418.

Lorsqu'une requête ETRN est reçue

...distribuer le courrier à l'IP de l'hôte ayant effectué la requête
Sélectionnez cette option pour que MDaemon envoie le courrier stocké à l'adresse IP de la machine qui a effectué la requête ETRN. La machine effectuant cette requête doit exécuter un serveur SMTP pour recevoir ces messages.

...distribuer le courrier au domaine suivant
Il s'agit du nom de l'hôte, du domaine ou de l'adresse IP auquel sera envoyé le courrier stocké lorsqu'une requête ETRN est reçue et honorée. L'ordinateur doit exécuter un serveur SMTP pour recevoir ces messages. Remarque : si vous indiquez un nom de domaine, les enregistrements A et MX peuvent être utilisés, en fonction des résultats des requêtes DNS lors de la distribution. Si vous souhaitez distribuer les messages à un hôte spécifique, indiquez son nom entre crochets (par ex. : [hote1.exemple.net]) ou indiquez l'adresse IP au lieu du nom de domaine.

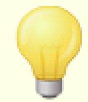
Si le domaine ci-dessus est local, le traiter comme un domaine inconnu
Activez cette option si le domaine est local mais que vous voulez que son courrier soit transmis comme s'il était distant.

Distribuer le courrier sur le port TCP
Indiquez le port sur lequel le courrier du domaine sera transmis.

ATRN

Cette passerelle accepte les requêtes ATRN
Activez cette option si vous voulez que MDaemon réponde aux commandes ATRN depuis le domaine pour lequel MDaemon agit comme passerelle. ATRN est une commande ESMTP utilisée dans On-Demand Mail Relay (ODMR) 51, qui est actuellement la meilleure méthode de relais disponible pour l'hébergement de courrier. Elle est supérieure à ETRN et aux autres méthodes, car elle requiert l'authentification avant que le courrier ne sorte de la file d'attente et ne requiert pas une adresse IP statique puisque le flux de données entre MDaemon et le domaine client est immédiatement inversé et que les messages sont transmis sans connexion —contrairement à ETRN qui utilise une connexion séparée après l'envoi de la commande ETRN. Cela permet aux domaines clients qui utilisent un compte à connexion téléphonique dynamique (non statique) de collecter leurs messages sans

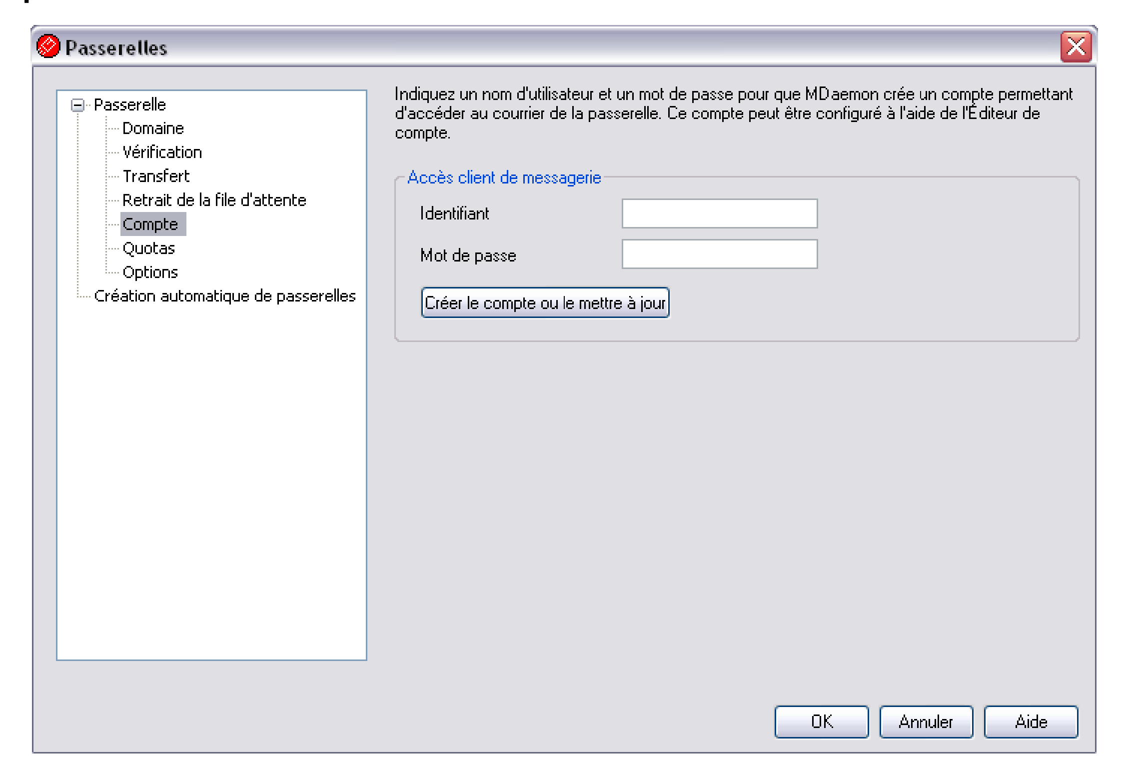
devoir utiliser POP ou DomainPOP pour qu'ils les distribuent à leurs utilisateurs car l'enveloppe SMTP d'origine est préservée.



ATRN requiert une session utilisant la commande AUTH. Les paramètres d'authentification se configurent dans l'onglet Options 418.

Autoriser une seule session ATRN à la fois
Cochez cette case si vous ne souhaitez pas autoriser plusieurs sessions ATRN simultanées.

7.1.1.5 Compte

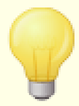


Cet onglet permet de créer un compte MDaemon associé à la passerelle. Ce compte peut ensuite être utilisé par un client ou serveur de messagerie pour se connecter à MDaemon et collecter les messages de la passerelle via IMAP, DomainPOP ou POP3. Le protocole IMAP est disponible uniquement avec MDaemon PRO.

Identifiant
Saisissez l'identifiant que le client utilisera pour accéder aux messages stockés dans sa boîte aux lettres.

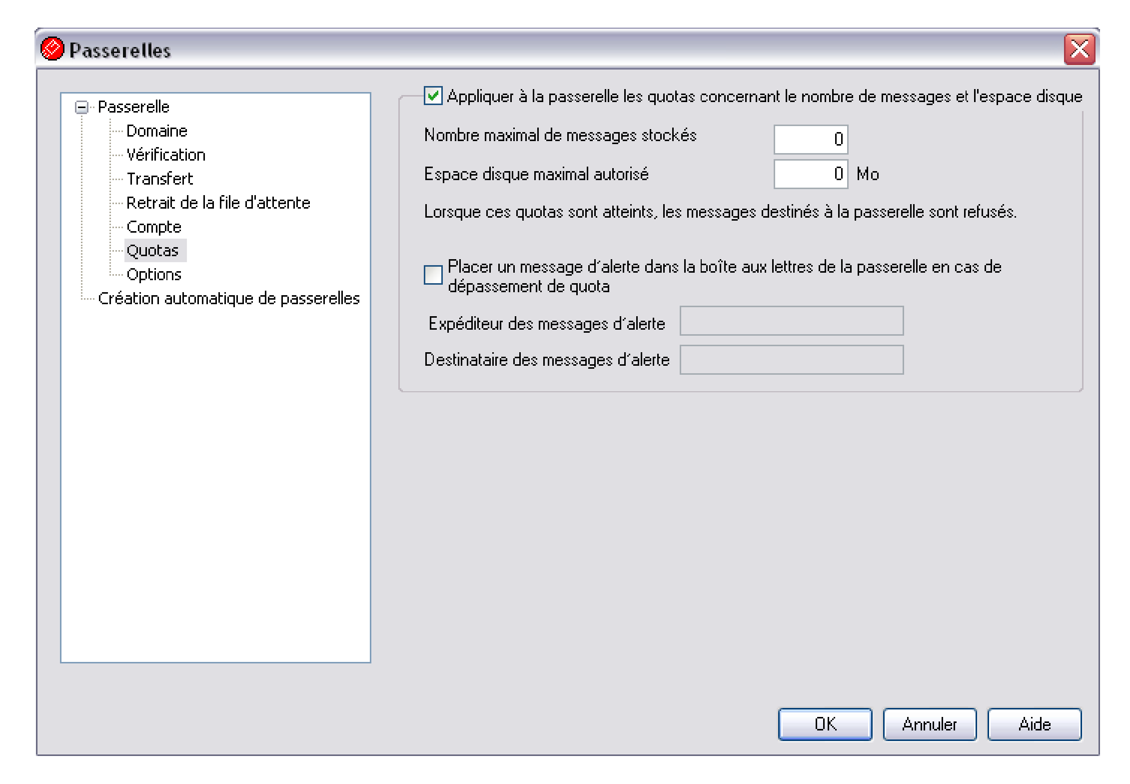
Mot de passe
Mot de passe de la boîte aux lettres.

Créer le compte ou le mettre à jour
Cliquez ici pour créer un compte ou mettre à jour l'identifiant et le mot de passe si le compte est déjà existant.



Vous pouvez modifier complètement (et même supprimer) un compte à l'aide de l'Éditeur de compte. Soyez attentif si vous effacez un compte car cela supprime le courrier et les répertoires de fichiers du compte – qui peuvent être ceux que la passerelle utilise.

7.1.1.6 Quotas



Quotas

Appliquer à la passerelle les quotas concernant le nombre de messages et l'espace disque
Activez cette option si vous souhaitez appliquer l'un des quotas ci-dessous à la passerelle. Ces quotas incluent les pièces jointes du répertoire Files. Lorsque l'un des quotas désignés est atteint, les messages entrants destinés à ce domaine sont refusés.

Nombre maximal de messages stockés
Nombre maximal de messages conservés par MDaemon pour cette passerelle. Saisissez "0" si vous ne souhaitez pas limiter le nombre de messages.

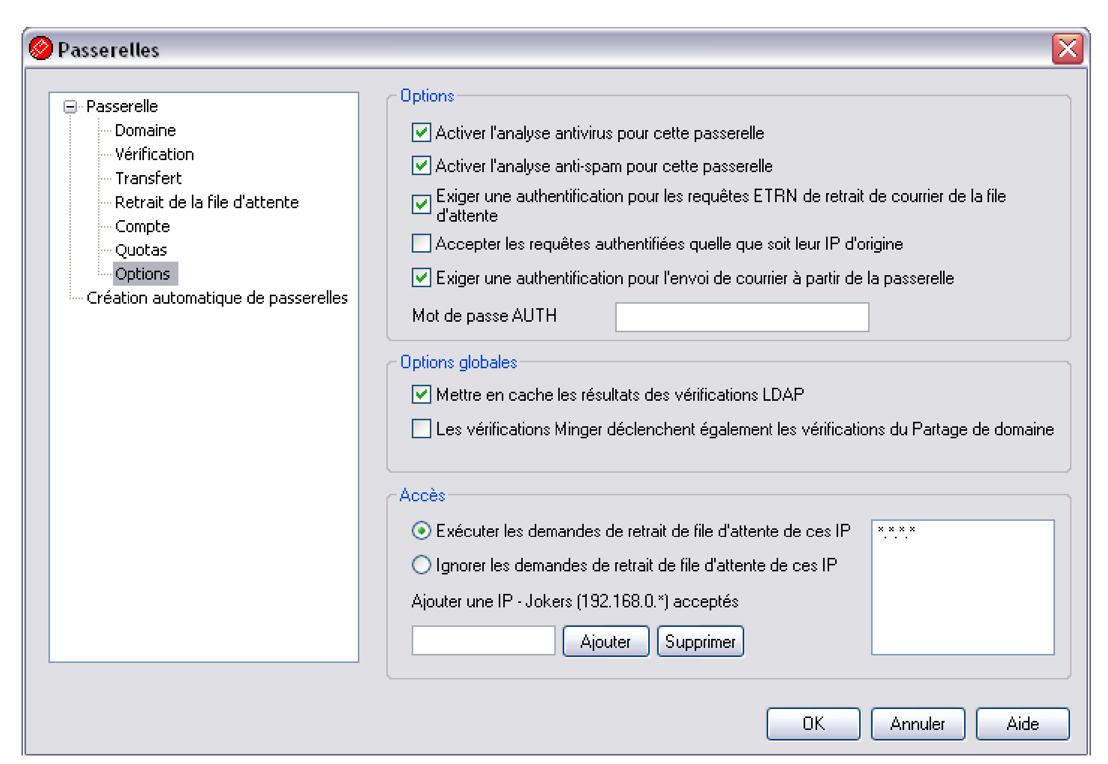
Espace disque maximal autorisé
Espace disque maximal attribué à cette passerelle. Saisissez "0" si vous ne souhaitez pas limiter l'espace disque.

Placer un message d'alerte dans la boîte aux lettres de la passerelle en cas de dépassement de quotas
Si cette option est activée et qu'une tentative de distribution du courrier au domaine a lieu et pourrait dépasser les limites de messages ou d'espace disque, le message sera transféré à l'adresse indiquée et accompagné d'un message d'avertissement approprié

Expéditeur des messages d'alerte
Indiquez ici l'adresse depuis laquelle le message d'avertissement de dépassement de quota sera envoyé.

Destinataire des messages d'alerte
Indiquez l'adresse à laquelle sera envoyé le message d'avertissement de dépassement de quota.

7.1.1.7 Options



Options

Activer l'analyse antivirus pour cette passerelle
Sélectionnez cette option si vous avez installé SecurityPlus for MDaemon et que vous souhaitez que les messages de cette passerelle de domaine soient analysés. Si vous décochez cette option, les messages ne sont pas analysés par SecurityPlus.

Activer l'analyse anti-spam pour cette passerelle
Sélectionnez cette option pour que les paramètres du Filtre anti-spam s'appliquent aux messages de cette passerelle de domaine. Sinon, ces messages seront exclus de l'analyse anti-spam.

Exiger une authentification pour les requêtes ETRN de retrait de courrier de la file d'attente
Si vous acceptez les requêtes ESMTP ETRN (onglet Retrait de la file d'attente), cette option est activée par défaut afin d'exiger l'authentification de l'hôte à l'aide de la commande ESMTP AUTH. Dans ce cas, vous devez indiquer un mot de passe dans le champ *Mot de passe AUTH*.

Décochez cette option si vous ne souhaitez pas exiger l'authentification des hôtes effectuant des requêtes ETRN.

Accepter les requêtes authentifiées quelle que soit leur IP d'origine
Si cette option n'est pas activée, seules les requêtes provenant d'adresses IP figurant dans la partie Accès sont acceptées.

Exiger une authentification pour l'envoi de courrier à partir de la passerelle
Avec cette option, si un message "prétend" provenir de ce domaine, il doit utiliser une session authentifiée (ou se connecter avec une adresse IP autorisée). Cette option est activée par défaut.

Lorsqu'une nouvelle passerelle est créée, cette option est activée par défaut. Si vous souhaitez qu'elle soit désactivée par défaut, modifiez le fichier `MDaemon.ini` comme suit :

`[Special]`
`GatewaySendersMustAuth=No` (par défaut : `Yes`)

Mot de passe AUTH
Si vous autorisez les requêtes ATRN, ou que l'option *Exiger une authentification pour les requêtes ETRN...* est activée, indiquez dans ce champ le mot de passe AUTH de la passerelle.



L'identifiant doit être le nom de domaine pour lequel MDaemon fait office de passerelle. Par exemple, si la passerelle "exemple.com" utilise ATRN pour retirer son courrier de la file d'attente, elle doit s'authentifier avec l'identifiant "exemple.com" et le mot de passe indiqué ci-dessus.

Options globales

Les deux options suivantes s'appliquent à toutes les passerelles.

Mettre en cache les résultats des vérifications LDAP
Activez cette option si vous souhaitez mettre en cache les résultats des vérifications409 LDAP pour les adresses.

Les vérifications Minger déclenchent également les vérifications du Partage de domaine
Si vous utilisez la méthode de vérification "Minger", cette option permet permet d'interroger vos hôtes de partage de domaine57 en plus du serveur Minger indiqué dans l'onglet Vérification409.

Accès

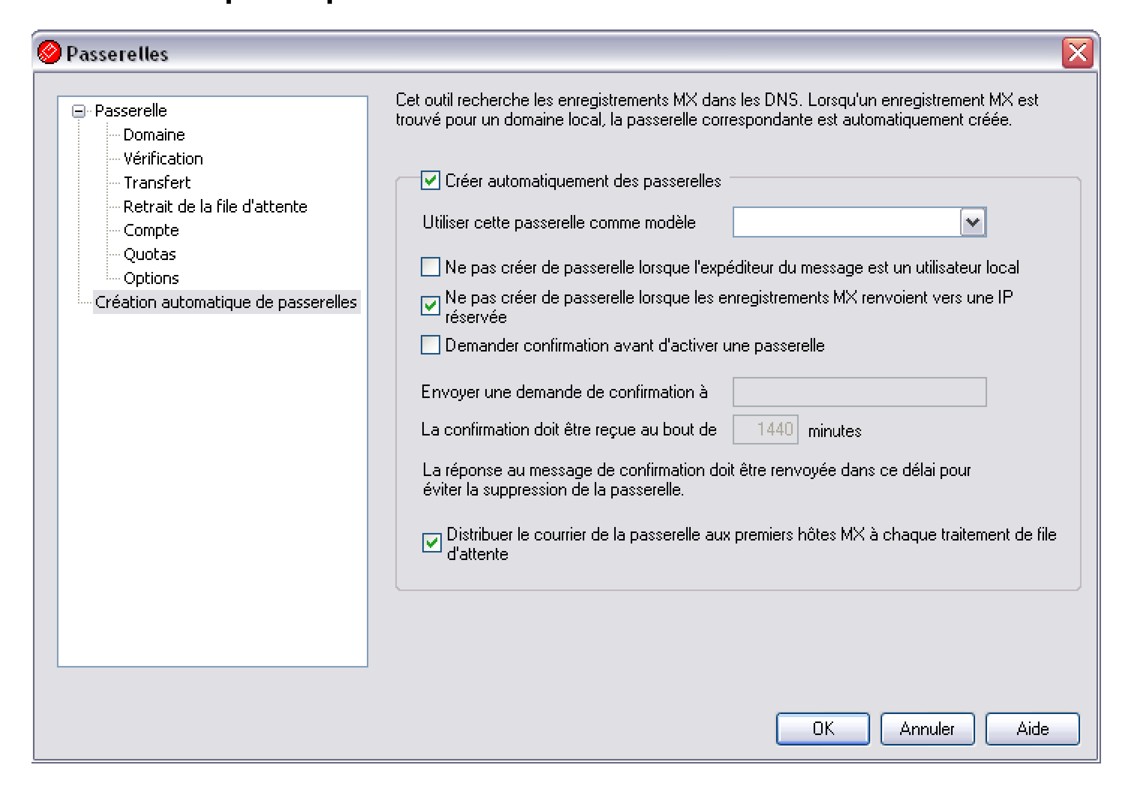
Exécuter les demandes de retrait de file d'attente de ces IP
Sélectionnez cette option pour que MDaemon exécute les requêtes ETRN/ATRN provenant des IP figurant dans la liste.

Ignorer les demandes de retrait de file d'attente de ces IP
Sélectionnez cette option pour que MDaemon ignore les requêtes ETRN/ATRN provenant des IP figurant dans la liste.

Ajouter une IP
Pour ajouter une IP à la liste, il suffit de la saisir dans le champ et de cliquer sur *Ajouter*.

Supprimer
Pour supprimer une IP de la liste, sélectionnez-la et cliquez sur ce bouton.

7.1.2 Création automatique de passerelles



Création automatique de passerelles (MDaemon PRO uniquement)

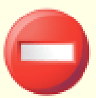
Cette fonctionnalité permet de créer automatiquement une passerelle pour un domaine auparavant inconnu lorsqu'une autre source tente de distribuer les messages de ce domaine à MDaemon, et qu'une requête DNS répertorie l'emplacement de MDaemon comme un enregistrement MX valide.

Par exemple :

Lorsque la création automatique de passerelles est activée, si l'adresse IP du domaine par défaut de MDaemon est 1.2.3.4 et qu'un message est distribué via SMTP pour un domaine inconnu exemple.com, MDaemon effectue des requêtes sur les enregistrements MX et A sur exemple.com pour voir si 1.2.3.4 est un hôte de relais de courrier connu pour lui. Si les résultats des requêtes DNS montrent que l'adresse IP de MDaemon est un hôte MX valide pour exemple.com, MDaemon crée alors automatiquement une nouvelle passerelle de domaine pour lui et acceptera ses messages. Les messages pour exemple.com seront alors stockés dans un dossier spécifique, et, si vous le souhaitez, transmis à des hôtes MX d'un niveau supérieur à chaque intervalle de traitement du courrier distant. Cette fonctionnalité permet donc de jouer le rôle de serveur secondaire pour un autre domaine en configurant simplement le système DNS pour qu'il utilise votre IP plutôt qu'un autre hôte MX.

Afin de sécuriser cette fonctionnalité, MDaemon peut être configuré pour envoyer une requête de confirmation à l'adresse électronique de votre choix. Pendant que MDaemon attend la réponse de confirmation, les messages pour le domaine seront acceptés et stockés mais ne seront pas distribués. Il est nécessaire de répondre aux requêtes de confirmation pendant le laps de temps que vous avez indiqué, sinon la passerelle créée automatiquement et tous les messages stockés seront supprimés. Si la confirmation est

reçue avant que ce laps de temps n'expire, les messages stockés seront distribués normalement.



Il est possible qu'une personne malintentionnée ou un spammeur tente d'exploiter cette fonctionnalité en configurant ses DNS pour qu'ils répertorient vos adresses IP de MDaemon comme l'un de leurs hôtes MX. La création automatique de passerelles doit par conséquent être utilisée avec précaution. Pour éviter une possible exploitation de cette fonctionnalité, il est recommandé d'activer l'option *Demander confirmation avant d'activer la passerelle*.

Créer automatiquement des passerelles
Activez cette option si vous voulez que MDaemon crée automatiquement des passerelles de domaine en fonction des résultats des requêtes DNS.

Utiliser cette passerelle comme modèle
Sélectionnez une passerelle de domaine dans ce menu déroulant et MDaemon utilisera ses paramètres comme modèle pour toutes les passerelles créées automatiquement dans le futur.

Ne pas créer de passerelle lorsque l'expéditeur du message est un utilisateur local
Activez cette option si vous ne voulez pas que les messages provenant d'utilisateurs locaux déclenchent la création automatique de passerelle.

Ne pas créer de passerelle lorsque les enregistrements MX renvoient vers une IP réservée
Cochez cette option si vous souhaitez empêcher la création automatique d'une passerelle lorsque les enregistrements MX renvoient vers une adresse IP réservée, de type 127.*, 192.*, etc.

Demander confirmation avant d'activer une passerelle
Lorsque cette option est activée, MDaemon envoie un message de confirmation à l'adresse électronique de votre choix afin de déterminer si la passerelle créée automatiquement est valide ou non. MDaemon continuera d'accepter les messages pour le domaine en question mais ne les distribuera que lors de la réception de la confirmation.

Envoyer une demande de confirmation à
Saisissez l'adresse e-mail à laquelle les messages de confirmation seront envoyés.

La confirmation doit être reçue au bout de X minutes
Indiquez le nombre de minutes pendant lesquelles MDaemon attend la réponse à un message de confirmation. Si ce laps de temps expire, la passerelle de domaine créée automatiquement est alors supprimée.

Distribuer le courrier de passerelle aux premiers hôtes MX à chaque traitement de file d'attente

Si vous voulez que MDaemon tente de distribuer les messages de cette passerelle à des hôtes MX supérieurs à chaque traitement de la file d'attente distante, activez alors cette option.

Voir également :

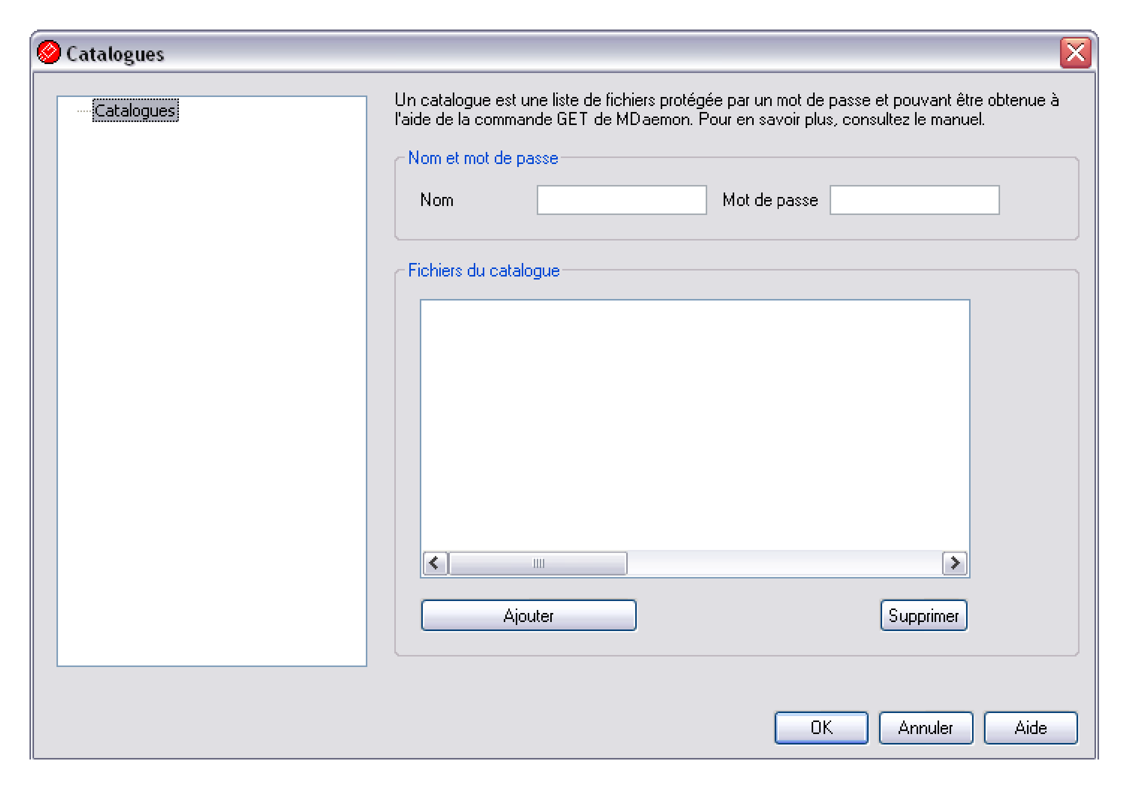
Passerelles de domaine 406
Éditeur de passerelle 407



Section VIII

8 Menu Catalogues

8.1 Éditeur de catalogue



Cliquez sur Catalogues » Nouveau catalogue... ou Catalogues » Modifier un catalogue... pour ouvrir l'Éditeur de catalogue. Avec les catalogues, les utilisateurs peuvent envoyer des requêtes afin que les fichiers qu'ils contiennent soient encodés et leur soient envoyés par e-mail.

Pour cela, l'administrateur attribue des "noms magiques" (raccourcis) à des fichiers sur disque. Les noms magiques sont similaires aux alias et indiquent un fichier spécifique situé sur un emplacement accessible à MDaemon. Les utilisateurs peuvent alors utiliser un type de message spécial pour requérir le fichier à l'aide du nom magique. Le format de ce message spécial est décrit dans la section Contrôle à distance du serveur 452 (voir commande **GET** dans Contrôle des listes de diffusion et des catalogues 454.

Nom et mot de passe

Nom
Saisissez le nom du catalogue.

Mot de passe
Saisissez un mot de passe pour ce catalogue.



Il n’est pas nécessaire de fournir un mot de passe pour tous les catalogues. Vous pouvez décider de rendre vos catalogues accessibles sans mot de passe.

Voir également :

Contrôle des listes de diffusion et des catalogues 454

Fichiers du catalogue

Liste des fichiers que contient le catalogue et leurs "noms magiques".

Supprimer
Pour supprimer un fichier du catalogue, sélectionnez-le et cliquez sur ce bouton.

Ajouter
Cliquez sur ce bouton pour ajouter un fichier dans le catalogue. Après avoir choisi le fichier que vous souhaitez ajouter, vous devrez fournir le "Nom magique" que vous voulez lui attribuer.

Le catalogue PUBLIC

Le catalogue PUBLIC est une exception aux règles normales qui contrôlent l’accès aux catalogues. En général, pour accéder à un catalogue, il est nécessaire de fournir un mot de passe qui a été attribué au catalogue. Avec le catalogue PUBLIC, le mot de passe n’est pas exigé. Les fichiers répertoriés dans le catalogue PUBLIC sont accessibles à tous ceux qui connaissent le nom magique du fichier.

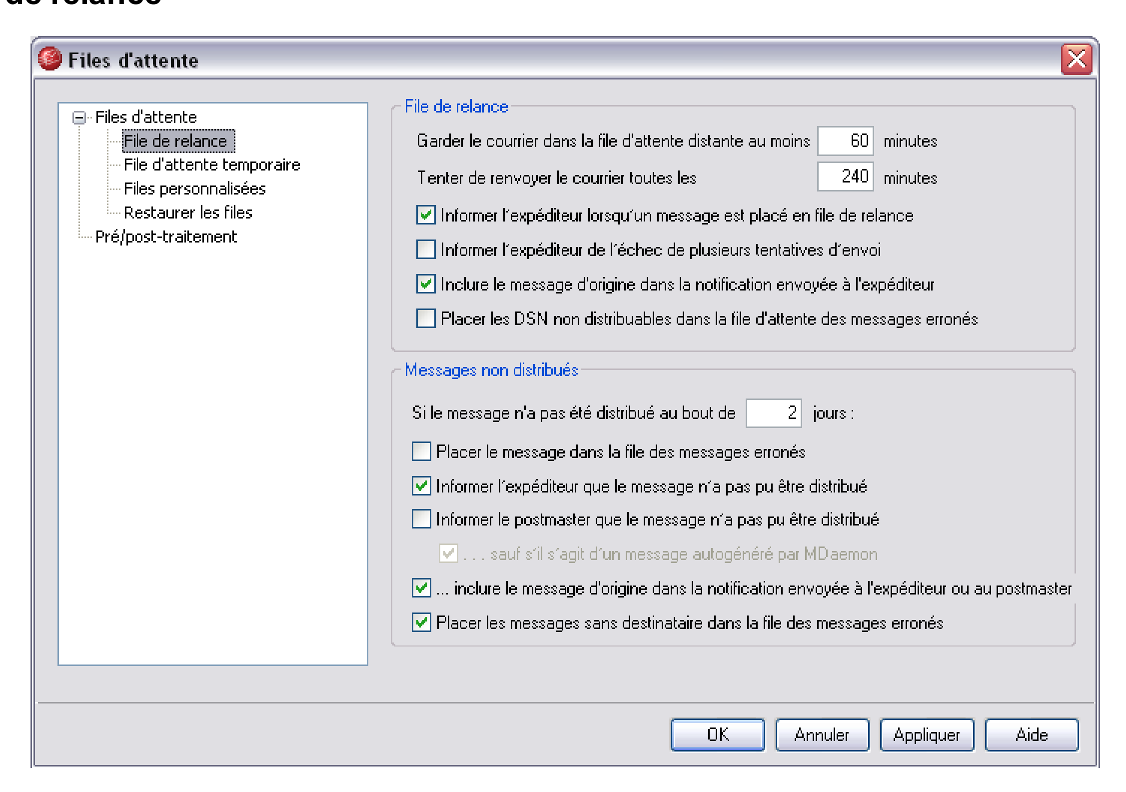


Section IX

9 Menu Files d'attente

9.1 Files d'attente

9.1.1 File de relance



Pour accéder à ces paramètres, cliquez sur Files d'attente » File de relance. Ils déterminent le "sort" des messages n'ayant pas pu être distribués suite à une erreur non fatale de distribution (par exemple si le serveur destinataire est temporairement indisponible).

File de relance

Garder le courrier dans la file d'attente distante au moins X minutes
Ce paramètre régit la durée pendant laquelle un message reste dans la file d'attente distante avant d'être supprimé et placé dans la file de relance. En général, les tentatives de distribution du courrier de la file distante sont plus rapides et plus fréquentes que celles de la file de relance.

Tenter de renvoyer le courrier toutes les X minutes
Ce paramètre détermine la fréquence de traitement des messages présents dans la file de relance.

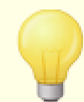
Informer l'expéditeur lorsqu'un message est placé en file de relance
Ce paramètre permet de signaler à l'expéditeur que son message est supprimé et placé en file de relance. Il est possible de consulter (ou modifier) le texte de ce message dans le fichier `DeliveryWarning.dat` situé dans le répertoire `\app\` de

MDaemon.

Informer l’expéditeur de l’échec de plusieurs tentatives d’envoi
Si une tentative d’envoi de courrier de la file de relance a échoué, l’expéditeur recevra un message lui expliquant la situation. Il est possible de consulter (ou modifier) le texte de ce message dans le fichier `DeliveryWarning.dat` situé dans le répertoire `\app\` de MDaemon.

Inclure le message d’origine dans la notification envoyée à l’expéditeur
En cochant cette case, le message d’origine est inclus sous forme de pièce jointe dans la notification envoyée à l’expéditeur.

Placer les DSN non distribuables dans la file d’attente des messages erronés
Cochez cette case si vous souhaitez que les notifications de distribution (DSN) ne pouvant pas être envoyées soient placées dans la file d’attente des messages erronés plutôt que d’effectuer une autre tentative.



Cela ne s’applique qu’aux DSN générées par MDaemon.

Messages non distribués

Si le message n’a pas été distribué au bout de X jours
Ce paramètre détermine le nombre de jours pendant lequel un message peut rester dans la file de relance avant d’être supprimé. Si vous indiquez la valeur "0" le message sera abandonné après la première tentative.

Placer le message dans la file des messages erronés
En cochant cette case, si un message n'a pas pu être distribué dans la limite de temps indiquée ci-dessus, il est déplacé dans le répertoire des messages erronés.

Informer l’expéditeur que le message n’a pas pu être distribué
Si un message n'a pas pu être distribué dans la limite de temps indiquée ci-dessus, MDaemon envoie une notification à l’expéditeur, lui signalant que ce message a été définitivement supprimé du serveur. Il est possible de consulter (ou modifier) le texte de ce message dans le fichier `DeliveryError.dat`.

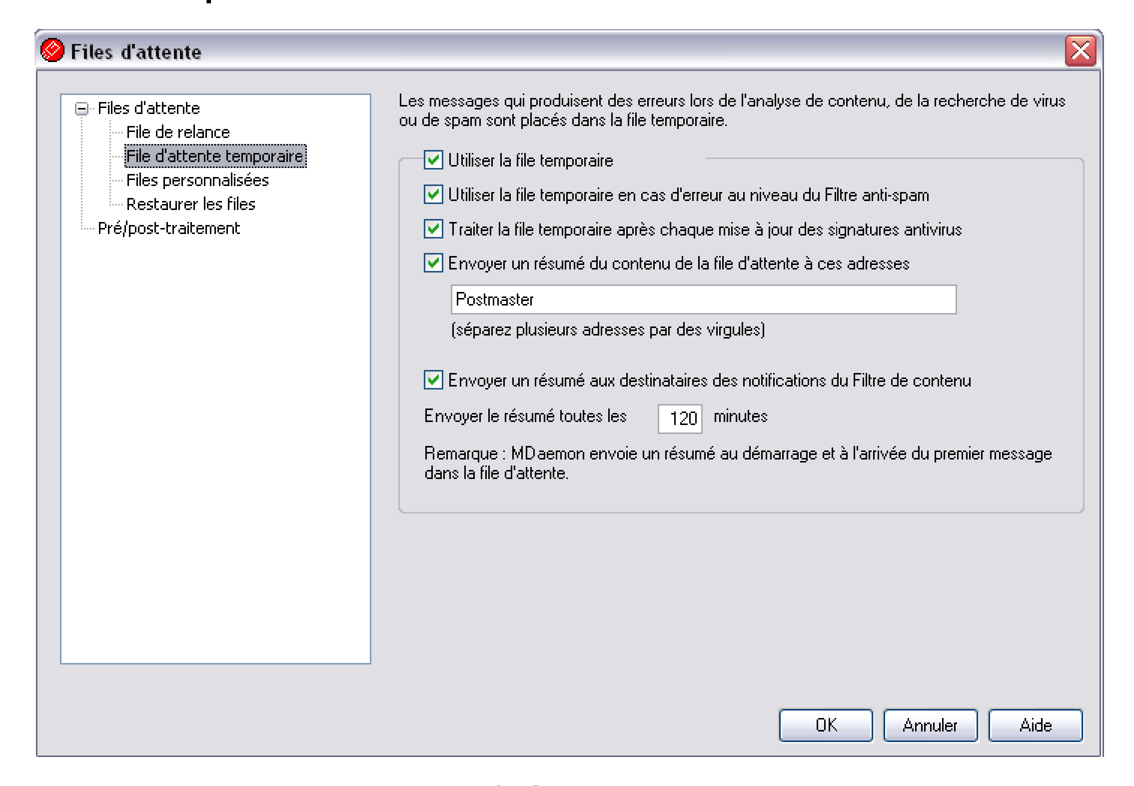
Informer le postmaster que le message n’a pas pu être distribué
En cochant cette case, le postmaster est averti de la suppression définitive d’un message du système de relance.

. . . sauf s’il s’agit d’un message autogénéré par MDaemon
Le système de relance n’avertit jamais MDaemon lorsqu’un message autogénéré ne parvient pas à être distribué. Toutefois, de telles informations peuvent être utiles au postmaster, c’est pourquoi il est informé lorsque ces messages ne peuvent pas être acheminés. Si vous ne voulez pas que le postmaster soit averti, cochez cette case. Les messages autogénérés peuvent être des notifications, des accusés de réception, des messages de réponse automatique, des résultats de traitement de compte, etc.

Inclure le message d’origine dans la notification envoyée à l’expéditeur ou au postmaster
En cochant cette case, le message d’origine est inclus sous forme de pièce jointe dans la notification envoyée à l’expéditeur ou au postmaster.

Placer les messages sans destinataire dans la file des messages erronés
Lorsque cette option est activée, les messages sans destinataire sont placés dans la file des messages erronés. Lorsqu'elle est désactivée, ils sont supprimés.

9.1.2 File d'attente temporaire



La file d'attente temporaire est destinée à recevoir les messages qui provoquent des erreurs lors du traitement antivirus, anti-spam ou de l'analyse de contenu. Si une erreur de logiciel se produit lors du traitement des messages, MDaemon les enregistre dans la file temporaire au lieu de les distribuer.

Ces messages demeurent dans la file tant que l'administrateur n'a pas pris de décision. Pour cela, le menu *Files d'attente* contient une option *Traiter la file temporaire*. Vous pouvez également effectuer un clic droit sur la file temporaire dans l'onglet *Statistiques* de l'interface principale et sélectionner *Remettre en file d’attente* : les messages seront alors acheminés dans la file distante ou locale pour être traités normalement. Si l'erreur qui est à l'origine de l'enregistrement des messages dans la file temporaire existe toujours, les messages sont replacés dans la file. Si vous souhaitez tout de même remettre les messages de la file temporaire à leurs destinataires sans tenir compte des problèmes risquant de se produire, effectuez un clic droit sur la file puis

cliquez sur "Distribuer". Au moment de la distribution, une fenêtre d'alerte vous rappelle que vous êtes sur le point d'introduire dans le flux de messages des e-mails dont le résultat du traitement antivirus, anti-spam ou de l'analyse de contenu est incorrect.

File temporaire

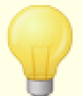
Utiliser la file temporaire
Lorsque cette case est cochée, les messages provoquant des erreurs lors du traitement antivirus ou de l'analyse de contenu sont transférés dans cette file.

Utiliser la file temporaire en cas d'erreur au niveau du Filtre anti-spam
Cochez cette case si vous souhaitez mettre en file temporaire les messages qui provoquent des erreurs au niveau du Filtre anti-spam.

Traiter la file temporaire après chaque mise à jour des signatures antivirus
Lorsque cette option est activée, la file temporaire est traitée automatiquement après chaque mise à jour des signatures de SecurityPlus for MDaemon. 177

Envoyer un résumé du contenu de la file d'attente à ces adresses
Cochez cette option si vous souhaitez envoyer, à intervalles réguliers, un résumé des messages de la file d'attente. Indiquez les adresses dans l'espace prévu à cet effet et séparez-les par des virgules.

Les messages de notification sont envoyés : au démarrage de MDaemon, la première fois qu'un message est transféré dans cette file, et aux intervalles définis dans l'option *Envoyer le résumé toutes les x minutes*.

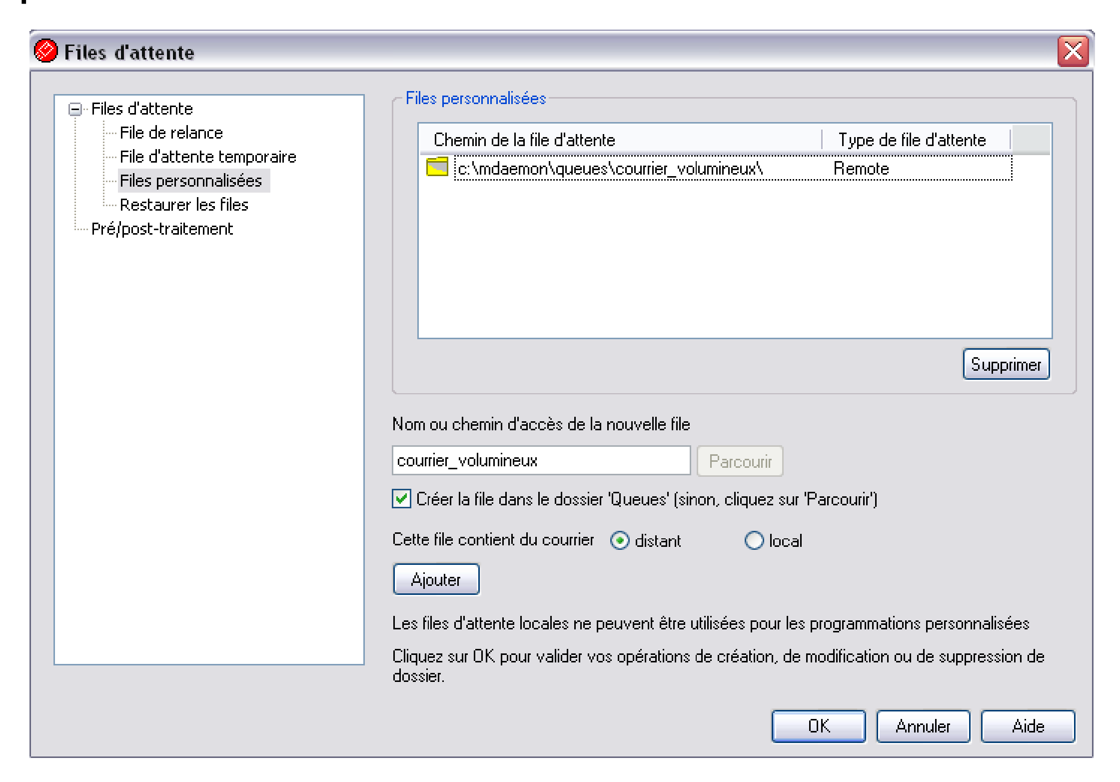


Si un message de notification provoque des erreurs de logiciel il risque de ne pas être distribué à tous les destinataires distants, mais il sera remis aux destinataires locaux.

Envoyer un résumé aux destinataires des notifications du Filtre de contenu
Envoie une copie de chaque message de notification aux adresses figurant dans l'onglet Destinataires 194 du Filtre de contenu.

Envoyer le résumé toutes les X minutes
Nombre de minutes écoulées avant que MDaemon envoie un message de notification aux adresses mentionnées ou aux destinataires des notifications du Filtre de contenu.

9.1.3 Files personnalisées

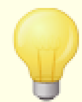


Cette boîte de dialogue se trouve dans Files d'attente » Files d'attente. Elle permet de créer des files d'attente de courrier local et distant. La prise en charge des files d'attente permet à MDaemon de surveiller plusieurs emplacements à partir desquels le courrier peut être envoyé. Vous pouvez créer de nouvelles files locales ou distantes et utiliser le Filtre de contenu pour que certains messages soient placés automatiquement dans vos files d'attente personnalisées. Les files distantes peuvent être associées à des programmations personnalisées dans le Programmateur d'événements 141.

Files personnalisées

Cette zone affiche la liste de vos files d'attente personnalisées avec leur chemin d'accès et indique si elles sont locales ou distantes.

Supprimer
Si vous souhaitez retirer une file d'attente de cette liste, sélectionnez-la, puis cliquez sur ce bouton.



Si vous supprimez une file personnalisée, toutes les programmations et règles du Filtre de contenu associées à cette file seront supprimées également.

Nom ou chemin d'accès de la nouvelle file
Saisissez dans ce champ le nom ou le chemin d'accès choisi pour cette file. Si vous souhaitez indiquer un chemin d'accès spécifique, vous devez décocher l'option *Créer la file dans le dossier Queues*. Si cette option n'est pas décochée, la file sera

automatiquement placée dans le dossier `\queues\`.

Créer la file dans le dossier Queues (sinon, cliquez sur Parcourir)
Si cette option est activée, la file d'attente est créée dans un sous-dossier du répertoire `\queues\` de MDaemon. Si vous la désactivez, elle est créée dans un sous-dossier du répertoire `\app\`, ou à l'emplacement de votre choix. Pour indiquer l'emplacement choisi cliquez sur *Parcourir* ou saisissez le chemin d'accès.

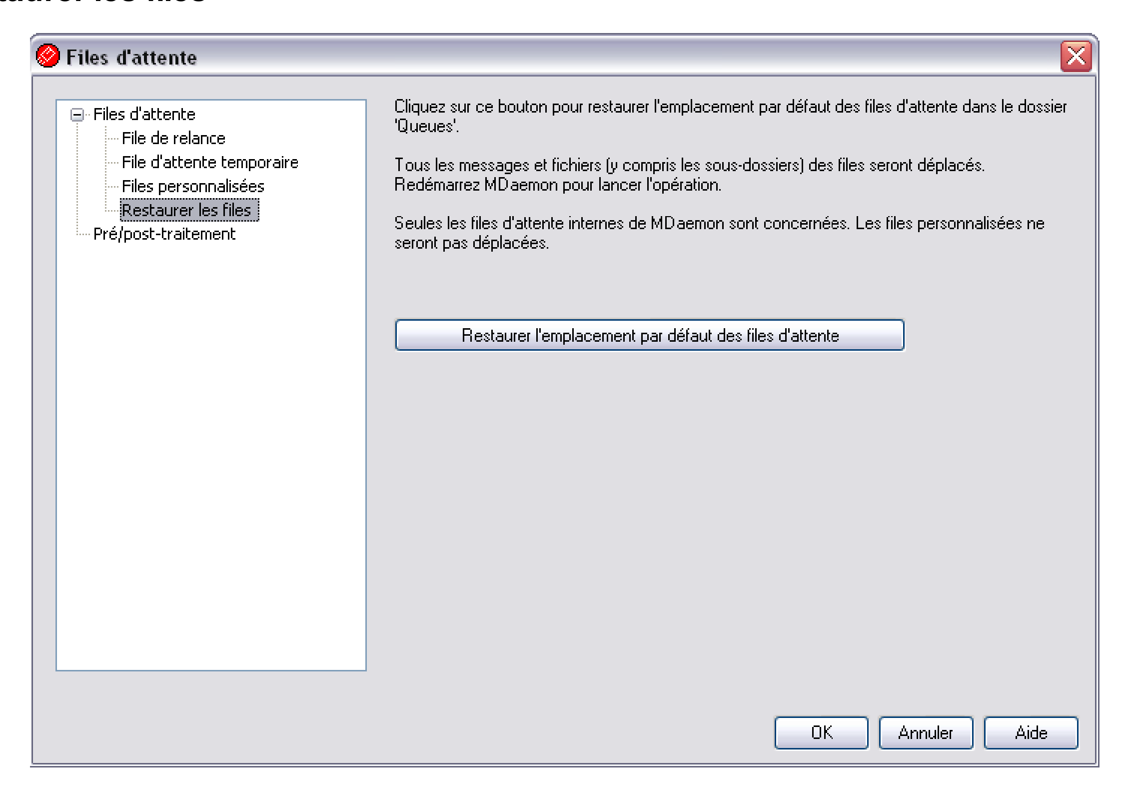
Cette file contient du courrier...

...distant
Sélectionnez cette option si vous voulez que la file d'attente soit utilisée pour le courrier distant.

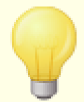
...local
Sélectionnez cette option si vous voulez que la file d'attente soit utilisée pour le courrier local.

Ajouter
Une fois que vous avez choisi le nom, l'emplacement et le type de la nouvelle file, cliquez sur le bouton *Ajouter* pour l'ajouter à la liste des files d'attente.

9.1.4 Restaurer les files

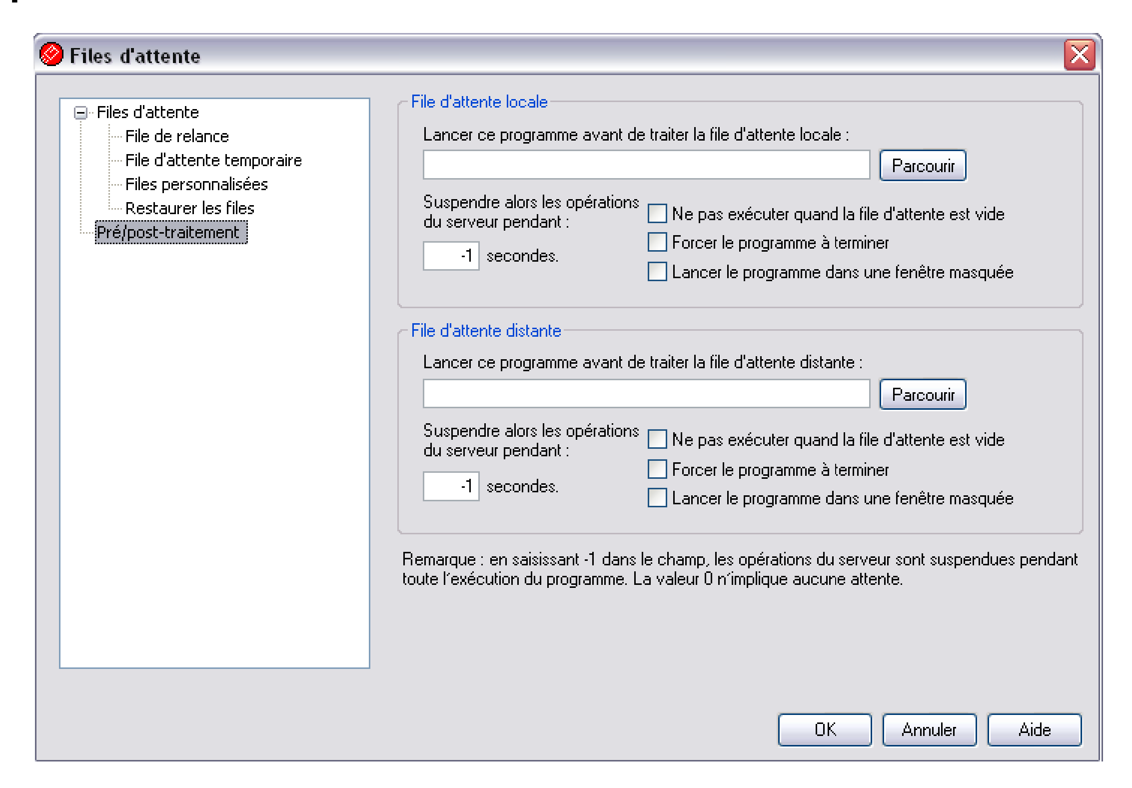


Restaurer l'emplacement par défaut des files d'attente
Par défaut, MDaemon enregistre le contenu des files d'attente (distante, locale, RAW...), dans le sous-dossier \MDaemon\Queues\, mais les versions précédentes utilisaient un autre emplacement. Il suffit de cliquer sur ce bouton pour que les files d'attente et les messages qui s'y trouvent soient déplacés de l'ancien dossier vers le nouveau. La modification ne sera prise en compte qu'après avoir redémarré MDaemon.



Les files personnalisées 434 ne seront pas déplacées par cette option.

9.2 Pré/post-traitement



Pré/post-traitement de la la file d'attente locale/distante

Lancer ce programme avant de traiter la file d'attente locale/distante
Ce champ indique le chemin et le nom d'un programme qui sera exécuté juste avant le traitement et la distribution de tous les messages RFC-2822 qui se trouvent dans la file d'attente locale ou distante. Si vous n'avez pas indiqué le chemin d'accès complet, MDaemon cherchera d'abord le fichier exécutable dans le répertoire MDaemon, puis dans le répertoire du système Windows, dans le répertoire Windows et, enfin, dans les dossiers répertoriés dans la variable de l'environnement PATH.

Suspendre alors les opérations du serveur pendant X secondes
La valeur saisie ici détermine le comportement de MDaemon lorsque le programme indiqué est en cours d'exécution. L'activité du serveur MDaemon peut être interrompue jusqu'à la fin du processus. Si celui-ci s'arrête avant la durée indiquée (en secondes), MDaemon reprend immédiatement son activité. Entrez la valeur zéro si vous ne souhaitez pas que le serveur suspende ses opérations. En saisissant "-1", il attendra la fin du programme, quelle que soit sa durée.

Ne pas exécuter quand la file d'attente est vide
Activez cette option si vous ne voulez pas que le programme indiqué s'exécute lorsque la file d'attente est vide.

Forcer le programme à terminer
Parfois, il est possible que le processus à exécuter ne s'arrête pas tout seul. Lorsque cette option est sélectionnée, MDaemon force la session à terminer une fois le temps indiqué dans *Suspendre les opérations du serveur pendant X secondes* écoulé. Ce paramètre ne fonctionne pas si l'intervalle de temps est défini à "-1".

Lancer le programme dans une fenêtre masquée
Activez cette option si vous souhaitez que le processus se lance dans une fenêtre masquée.

9.3 Gestionnaire de files d'attente et de statistiques

Pour accéder au Gestionnaire de files d'attente et de statistiques, cliquez sur Files d'attente » Gestionnaire de files d'attente et de statistiques. Il est composé de quatre onglets ("pages"). Chacune de ces pages a été conçue dans un but particulier tout en conservant le même format afin d'être plus facile à utiliser.

Page file d'attente 439

L'onglet par défaut est la Page file d'attente. Vous pouvez gérer facilement depuis cette page toutes les files d'attente de courrier standard de MDaemon ainsi que les dossiers de boîte aux lettres de compte utilisateur. En cliquant simplement sur la file d'attente ou l'utilisateur de votre choix, une liste de tous les fichiers de messages contenus dans la file d'attente indiquée s'afficheront ainsi que de nombreuses informations pertinentes concernant chaque message : l'expéditeur, le destinataire, le contenu de l'en-tête To:, l'objet du message, sa taille et le temps depuis lequel il se trouve à son emplacement actuel. De plus, des options vous permettent de copier ou de déplacer facilement des messages entre des dossiers, ou de les supprimer complètement.

Page utilisateur 442

Dans la Page utilisateur s'affiche la liste de tous les utilisateurs MDaemon. Cette liste inclut leur nom complet, le nom de la boîte aux lettres, le nombre de messages dans leur boîte, le total de l'espace disque que leur compte utilise, et la date à laquelle ils ont vérifié leur courrier pour la dernière fois. Cette liste peut également être sauvegardée sur disque sous forme de fichier texte ou dans un format délimité par des

virgules pour être utilisée avec des bases de données.

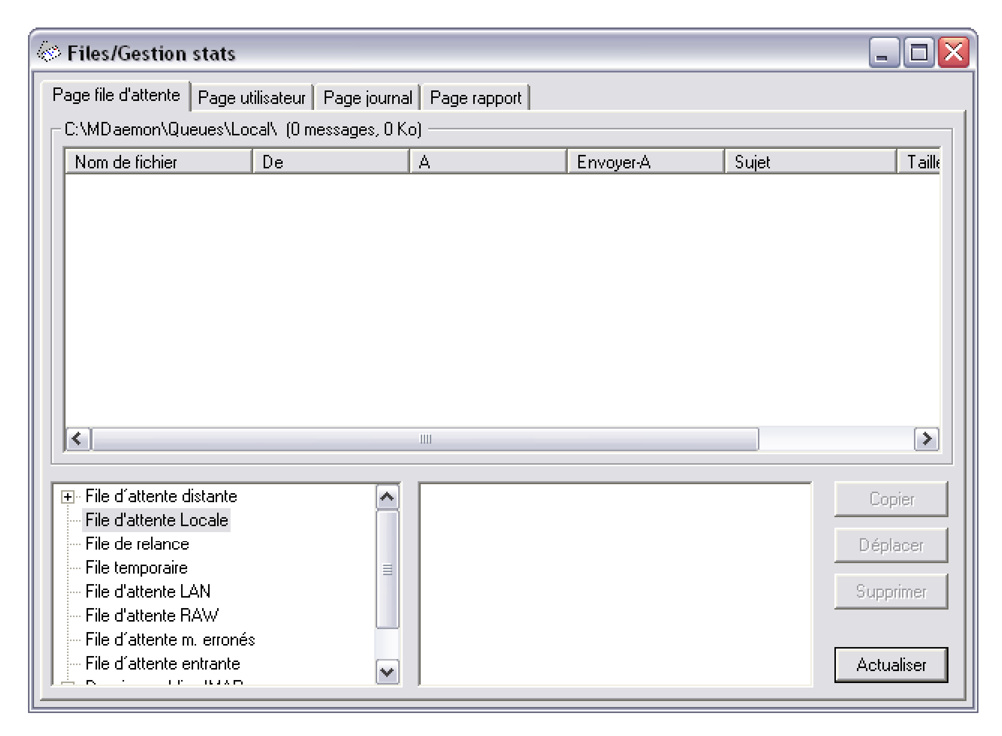
Page journal 444

Avec cette boîte de dialogue, vous pouvez afficher les fichiers journaux de MDaemon dans un format de liste simple. Cette fonctionnalité est particulièrement utile pour examiner rapidement l'historique des transactions de courrier de MDaemon car elle condense le fichier journal sélectionné dans une liste en colonnes qui contient : le type du message (POP entrant, DomainPOP, RFC2822, etc.), l'hôte auquel MDaemon se connecte durant la transaction, l'expéditeur, le destinataire, la taille du message, la date à laquelle le message a été traité, et si la transaction a été effectuée ou non avec succès. Vous pouvez également examiner la portion détaillée de l'audit concernant l'une des entrées de la liste en double-cliquant sur l'entrée souhaitée. La portion de l'audit dans laquelle la transaction a été effectuée s'affichera. Les audits affichés dans la Page journal peuvent être sauvegardés sous forme de fichier texte ou dans un format délimité par des virgules pour être utilisés avec des bases de données.

Page rapport 446

Le dernier onglet est la Page rapport. Grâce à cette fonctionnalité, vous pouvez produire un rapport contenant tous les paramètres de configuration de MDaemon en format lisible en texte non crypté. En raison du grand nombre de paramètres et de configurations optionnelles dans MDaemon, cela peut améliorer considérablement la vitesse de traitement des modifications de la configuration d'administration ainsi que permettre de diagnostiquer d'éventuels problèmes de configuration. En outre, ce rapport s'affiche dans un format texte modifiable, ce qui vous permet de copier/coller les informations qu'il contient ou d'ajouter des annotations ou d'autres informations dans le fichier avant de le sauvegarder.

9.3.1 Page file d'attente

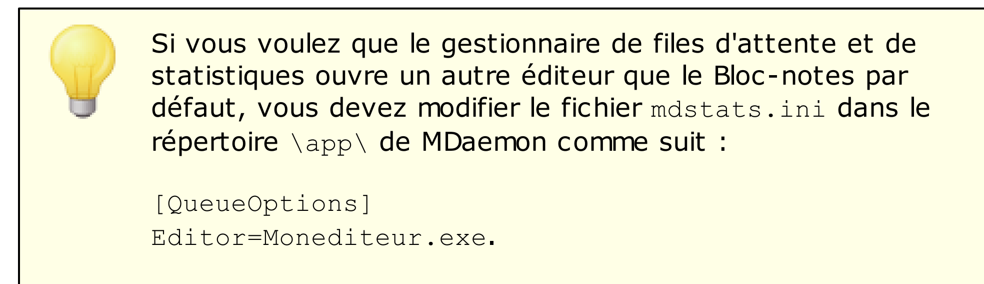


Lorsqu'une file d'attente ou un utilisateur est sélectionné dans la zone Files d'attente de messages ou dans la zone utilisateur à côté, une liste de tous les fichiers de messages contenus dans la file d'attente sélectionnée s'affiche dans la zone principale de cette page. Cette liste contient le nom de fichier de chaque message, l'expéditeur, le destinataire, le contenu de l'en-tête To:, l'objet du message, sa taille et la durée depuis laquelle il se trouve à son emplacement actuel (par date et heure).

Au-dessus de cette zone est indiqué le chemin complet vers le répertoire actuellement affiché, ainsi que le nombre de messages affichés et la taille de ce répertoire.

Vous pouvez copier, déplacer ou supprimer un ou plusieurs de ces fichiers en les sélectionnant dans la liste et en cliquant sur le bouton approprié sous celui-ci.

Le contenu de ces fichiers peut également être modifié directement. Double-cliquez simplement sur le fichier que vous souhaitez modifier (ou effectuez un clic droit sur son nom et sélectionnez "Modifier"). Le fichier s'ouvre alors dans le Bloc-notes de Windows.



Si vous voulez que le gestionnaire de files d'attente et de statistiques ouvre un autre éditeur que le Bloc-notes par défaut, vous devez modifier le fichier `mdstats.ini` dans le répertoire `\app\` de MDaemon comme suit :

```
[QueueOptions]
Editor=Monediteur.exe.
```

Si le fichier exécutable n'est pas au même emplacement,

indiquez son chemin d'accès.

Il est possible de naviguer dans cette zone à l'aide des barres de défilement vertical ou horizontal, ou vous pouvez cliquer n'importe où dans la zone et utiliser les flèches pour vous déplacer. Vous pouvez trier les informations contenues dans cette page selon la colonne de votre choix. En cliquant simplement sur la colonne souhaitée pour la trier par ordre croissant (A-Z, 1-2), ou en cliquant deux fois dessus pour la trier par ordre décroissant (Z-A, 2-1). Les colonnes peuvent également être redimensionnées en positionnant le curseur sur la ligne située entre les en-têtes de colonnes jusqu'à ce qu'elle change de forme, puis en faisant glisser la colonne jusqu'à la largeur de votre choix.

Sélectionner des fichiers

Sélection d'un fichier individuel Cliquez sur le fichier voulu.

Sélection de plusieurs fichiers contigus Cliquez sur le premier fichier que vous souhaitez sélectionner, tout en maintenant enfoncée la touche SHIFT, puis cliquez sur le dernier fichier dans la liste désirée.

Sinon, vous pouvez utiliser les touches FLECHES, ACCUEIL, FIN, HAUT et BAS, tout en maintenant enfoncée la touche MAJ pour sélectionner des fichiers contigus.

Sélection de plusieurs fichiers non contigus Cliquez sur les fichiers voulus dans la colonne Nom de fichier tout en maintenant enfoncée la touche CTRL.

Files d'attente de messages
Cliquez sur une entrée dans la fenêtre en bas à gauche pour afficher une liste de tous les fichiers contenus dans la file d'attente indiquée. Si vous cliquez sur *Dossiers utilisateurs*, une liste de tous les utilisateurs MDaemon s'affichera dans la boîte *Liste d'utilisateurs* à droite de la section Files d'attente de messages.

Liste des utilisateurs
Dans cette boîte s'affiche une liste de tous les utilisateurs MDaemon lorsque vous avez cliqué sur *Dossiers utilisateurs* dans la section Files d'attente de messages. Cliquez sur le nom d'un utilisateur pour afficher une liste de tous les fichiers de messages contenus actuellement sa boîte aux lettres.

Actualiser
Comme les files d'attente de courrier sont dynamiques quand MDaemon est actif – avec des fichiers de messages constamment en cours de transfert – vous pouvez cliquer régulièrement sur ce bouton pour actualiser la liste de fichiers que vous avez affichée.



Pour que les listes affichées soient automatiquement actualisées vous pouvez modifier le fichier `MDstats.ini` comme suit :

`[QueueOptions]`
`AutoRefresh=15` (dans ce cas, l'affichage s'actualise toutes les 15 secondes).

Si vous ne souhaitez pas que l'affichage s'actualise automatiquement, indiquez "0".

Copier
Lorsqu'un ou plusieurs fichiers sont sélectionnés, cliquez sur ce bouton pour copier les fichiers sélectionnés dans une autre file d'attente ou un dossier de boîte aux lettres d'un utilisateur. Après avoir cliqué sur ce bouton, la boîte de dialogue *Copier message(s)* s'ouvre pour que vous puissiez sélectionner l'emplacement dans lequel vous souhaitez que les fichiers sélectionnés soient copiés.

Déplacer
Lorsqu'un ou plusieurs dossiers sont sélectionnés, cliquez sur ce bouton pour déplacer les fichiers sélectionnés dans une autre file d'attente ou boîte aux lettres. Après avoir cliqué sur ce bouton, la boîte de dialogue *Déplacer message(s)* s'ouvre pour que vous puissiez sélectionner l'emplacement dans lequel vous souhaitez que les fichiers sélectionnés soient déplacés.



Les fichiers copiés ou déplacés vers d'autres files d'attente conservent rarement leurs noms de fichier d'origine. Afin d'éviter d'écraser des fichiers du même nom qui peuvent déjà se trouver dans la file d'attente, MDaemon évalue toujours la destination finale d'un nom de fichier en fonction du fichier HIWATER.MRK situé dans le dossier de destination.

Supprimer
Pour supprimer un fichier, sélectionnez-le et cliquez sur ce bouton (une fenêtre de confirmation s'affiche).



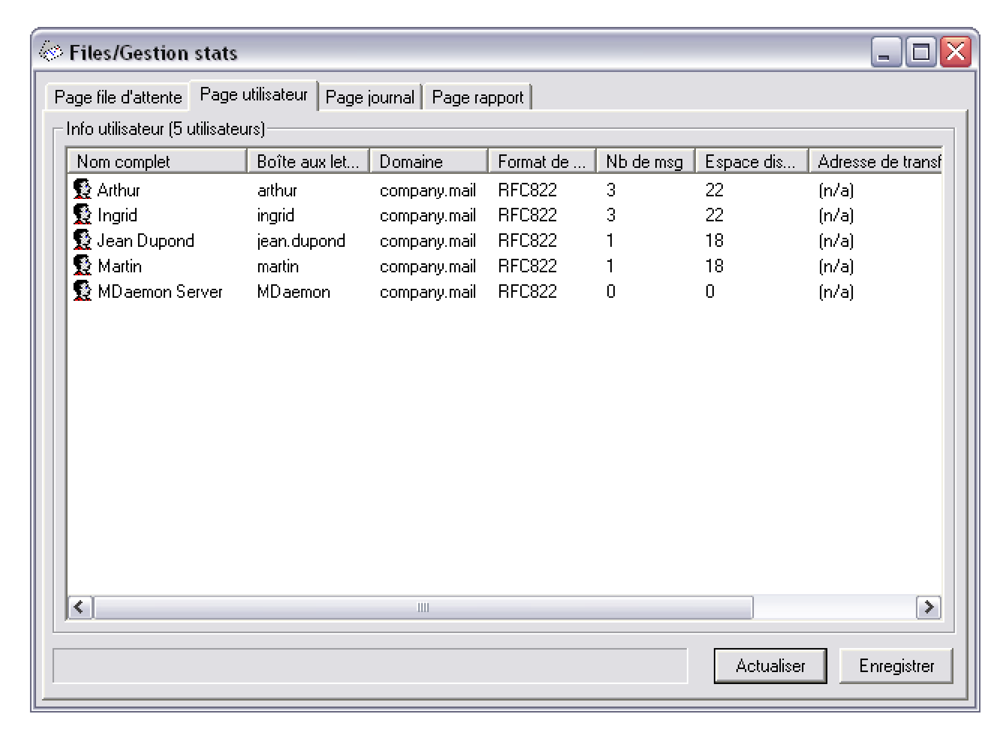
Les files d'attente de courrier sont dynamiques lorsque MDaemon est actif – avec des messages constamment en cours de transfert. Pour cette raison, sachez que lorsque vous copies, déplacez ou supprimez des fichiers, il est possible que MDStats vous avertisse que l'action que vous tentez n'a pas pu être terminée. Cela se produit lorsque le fichier de message avec *lequel* vous essayez de travailler a déjà été retiré par MDaemon avant le début de l'action souhaitée. En cliquant sur le bouton Actualiser, vous pouvez mettre à jour la liste des fichiers actuellement affichés dans cette zone.

Pour empêcher la sortie des messages de la liste d'attente lorsque vous les modifiez, apportez la modification suivante au fichier `MDstats.ini` :

```
[QueueOptions]
LockOnEdit=Yes.
```

Ainsi, un fichier LCK sera créé dès lors que vous modifiez un message, ce qui lui évitera d'être sorti de la file d'attente jusqu'à ce que vous ayez terminé.

9.3.2 Page utilisateur

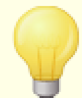


Info utilisateur

Lorsque vous choisissez la Page utilisateur, le gestionnaire de files d'attente et de statistiques charge immédiatement une liste de tous les comptes MDaemon dans la zone Infos utilisateur. Cette liste contient le nom complet de chaque utilisateur, le nom de sa boîte aux lettres, le domaine auquel le compte appartient, le nombre de messages qu'il contient, son format de courrier, le montant de l'espace disque (en octets) qu'occupe le compte, son adresse de transfert, et enfin la date à laquelle le courrier a été vérifié pour la dernière fois. Etant donné que les informations contenues dans cette liste changent constamment, il est possible de les mettre à jour facilement en cliquant sur le bouton *Actualiser*.

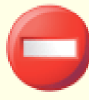
Il est possible de se déplacer dans cette zone à l'aide des barres de défilement horizontales et verticales, ou en cliquant dans cette zone et en utilisant les touches

FLÈCHES. Vous pouvez trier les informations contenues dans la zone Infos utilisateur en fonction de la colonne de votre choix. Cliquez une fois sur la colonne voulue pour la trier par ordre croissant (A-Z), ou cliquez deux fois pour la trier par ordre décroissant (Z-A). Il est également possible de les redimensionner en plaçant le curseur sur la ligne séparant les en-têtes de colonnes jusqu'à ce qu'elle change d'aspect, puis en la déplaçant jusqu'à la largeur souhaitée. De plus, vous pouvez double-cliquer sur une entrée pour que MDStats soit déplacé dans la Page file d'attente avec le contenu du dossier de boîte aux lettres.



Par défaut, cette liste affiche le Nombre de messages, et non le nombre de fichiers, et l'espace disque utilisé par les messages, et non l'espace utilisé par tous les fichiers dans le répertoire. Il s'agit des informations de Quota signalées par MDaemon. Il est également possible d'afficher le nombre de fichiers et l'espace disque utilisé par tous les fichiers et non par les messages. Pour cela, modifiez le fichier `MDstats.ini` comme suit :

```
[UserOptions]
ShowQuota=No.
```



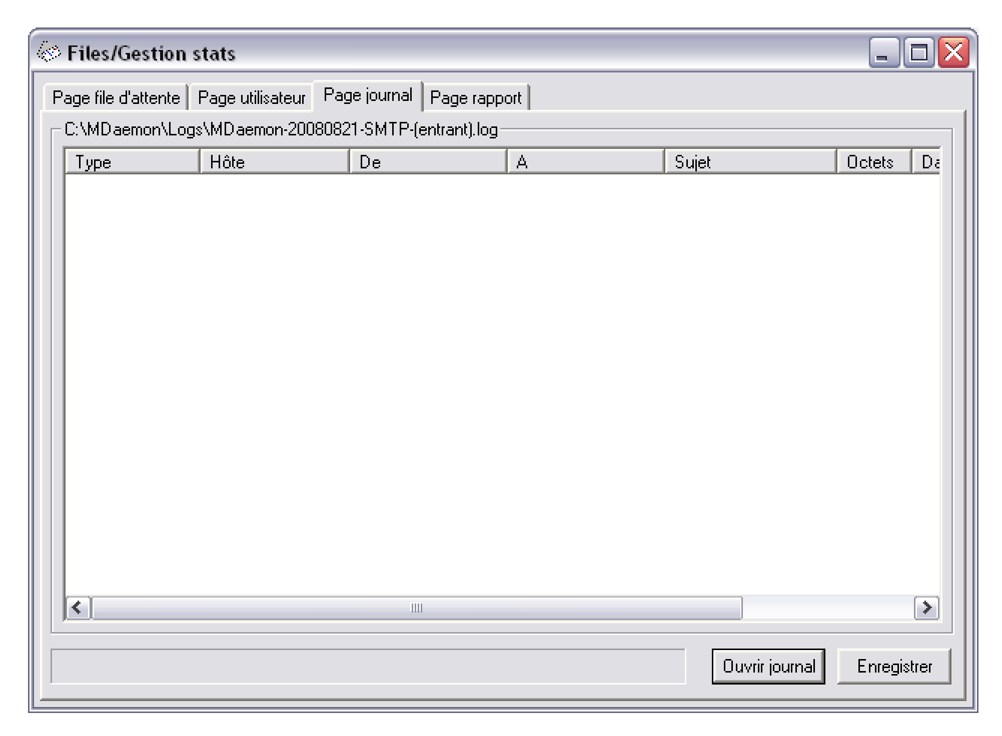
Les dossiers utilisateurs contiennent un ficher appelé "hiwater.mrk" que le gestionnaire de files d'attente et de statistiques lit pour déterminer certaines informations utilisateur. Évitez de supprimer ce fichier inutilement car MDStats ne pourrait plus obtenir certaines des informations répertoriées dans la liste Informations utilisateur.

Actualiser
Les statistiques utilisateurs comme le nombre de messages contenus dans sa boîte aux lettres et le montant de l'espace disque que leur compte utilise, changent constamment. Vous pouvez facilement mettre à jour les informations contenues dans la zone Informations utilisateur en cliquant sur le bouton *Actualiser*.

Indicateur de progression
Comme les listes Infos utilisateur peuvent parfois être de grande taille, un indicateur de progression indique que le programme est en cours de fonctionnement lorsque que des fichiers de grande taille sont chargés.

Enregistrer
Les informations contenues dans la zone Infos utilisateur peuvent être enregistrées sous forme de fichier dans un format délimité par des virgules afin de l'utiliser avec des bases de données, ou sous forme de fichier texte ASCII non crypté en cliquant sur le bouton *Enregistrer*.

9.3.3 Page journal



Cette page affiche les fichiers journaux détaillés de MDaemon que vous sélectionnez avec le bouton *Ouvrir journal*. Elle offre un moyen rapide pour examiner facilement l'historique des transactions de courrier que MDaemon a traitées sans avoir à trier le volume d'informations que les fichiers journaux de MDaemon peuvent parfois contenir. Lorsqu'un rapport de journal est affiché dans cette zone, le gestionnaire de files d'attente et de statistiques le décompose dans un format simple contenant le type de message (POP Entrant, DomainPOP, RFC2822, etc.), l'hôte auquel se connecte MDaemon lors de la transaction, l'expéditeur, le destinataire, la taille du message, la date à laquelle le message a été traité et si la transaction a été ou non effectuée avec succès.

Vous pouvez également étudier la partie détaillée du journal concernant les entrées de la liste en double-cliquant sur l'entrée voulue. La partie du journal dans laquelle la transaction a été effectuée s'affichera. À l'aide du menu de raccourcis disponible avec un clic droit, vous pouvez copier/coller la partie détaillée du journal dans un éditeur de texte pour l'enregistrer ou la modifier si vous le souhaitez.

Il est possible de se déplacer dans cette zone à l'aide des barres de défilement horizontales et verticales, ou en cliquant dans cette zone et en utilisant les touches FLÈCHES. Vous pouvez redimensionner les colonnes de cette zone en plaçant le curseur sur la ligne séparant les en-têtes de colonne jusqu'à ce qu'elle change d'aspect, puis en la déplaçant jusqu'à la largeur souhaitée.

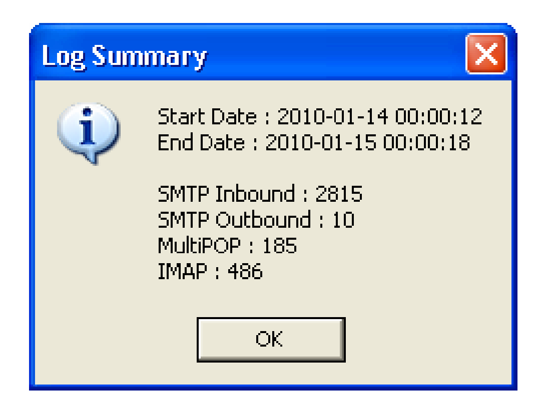


La page journal affiche les fichiers journaux compilés à l'aide des options *Enregistrer l'intégralité des sessions de courrier* ou *Enregistrer un résumé des sessions de courrier* (dans Configuration

» Domaine/serveurs par défaut » Journalisation » Mode de journalisation. Il est recommandé d'utiliser *Enregistrer l'intégralité des sessions de courrier*. En effet, si vous sélectionnez l'autre option, très peu d'informations seront affichées dans votre rapport de journal. Comme ce rapport condense lui-même le journal détaillé dans un affichage résumé de l'activité de MDaemon, tout en fournissant la possibilité de visualiser toutes les transactions lorsque cela est nécessaire (en double-cliquant sur une entrée), il n'est pas nécessaire que MDaemon résume le fichier journal lorsqu'il le compile.

Ouvrir journal
Cliquez sur ce bouton sélectionner le fichier journal que vous souhaitez examiner. Si vous cliquez sur ce bouton lorsqu'un fichier journal est déjà affiché, vous pouvez ajouter le nouveau fichier à celui qui est déjà affiché.

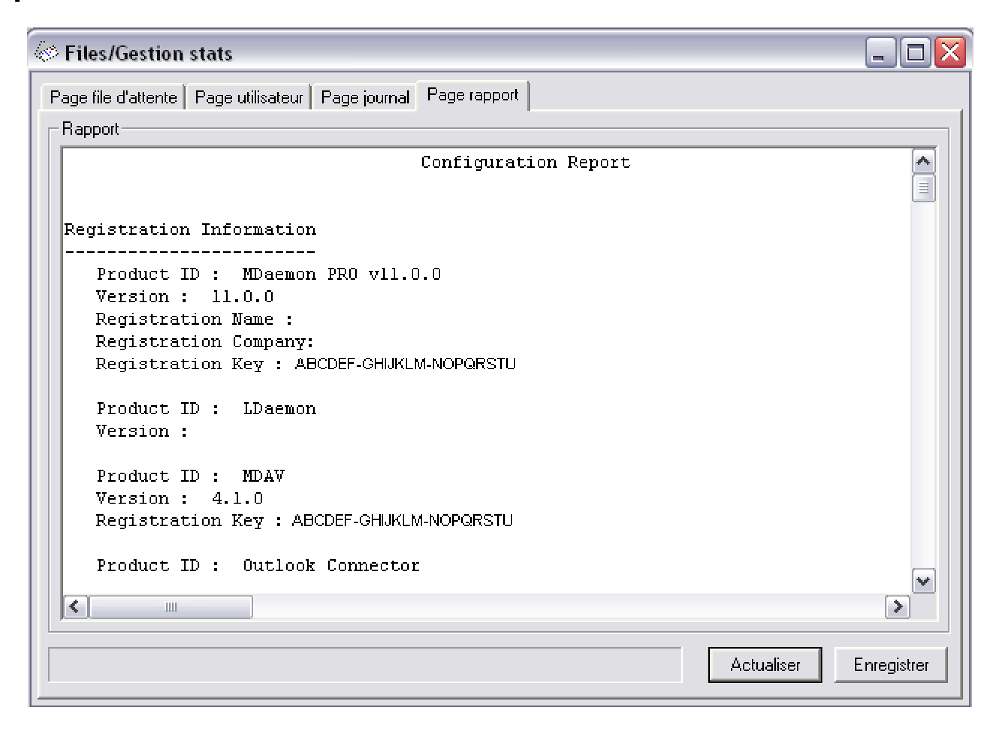
Après l'affichage d'un journal, une boîte de dialogue contenant le résumé du journal sélectionné s'ouvre. Lors de l'enregistrement d'un rapport de journal sous forme de fichier texte, un résumé du journal est ajouté.



Indicateur de progression
Comme les fichiers journaux peuvent parfois être volumineux, un indicateur de progression se trouve au bas de la page et indique que le programme est toujours en cours de fonctionnement lorsque que des fichiers de grande taille sont chargés ou enregistrés.

Enregistrer
Les informations contenues dans cette page peuvent être enregistrées sous forme de fichier dans un format délimité par des virgules afin de l'utiliser avec des bases de données, ou sous forme de fichier texte ASCII non crypté en cliquant sur le bouton *Enregistrer*.

9.3.4 Page rapport



Rapport
Rapport détaillé qui répertorie chaque paramètre de MDaemon dans un format de texte lisible facilement. Cette fonctionnalité diminue considérablement le temps nécessaire à l'administrateur pour vérifier les paramètres de configuration de MDaemon et permet de résoudre de probables problèmes de configuration.

Vous pouvez vous déplacer dans ce rapport à l'aide des barres de défilement ou des touches de curseur. De plus, la fenêtre *Rapport* est également un éditeur de texte, permettant ainsi d'insérer des annotations ou des informations supplémentaires dans le rapport avant de l'enregistrer dans un fichier.

Actualiser
Cliquez sur ce bouton pour mettre à jour les informations affichées.

Indicateur de progression
Tout comme dans les autres onglets, il existe dans la Page rapport un indicateur de progression montrant que le programme est toujours en cours de fonctionnement lorsque que des fichiers de grande taille sont chargés ou enregistrés.

Enregistrer
Cliquez sur ce bouton pour enregistrer le rapport actuellement affiché. Après avoir cliqué sur ce bouton, une boîte de dialogue *Enregistrer sous* s'ouvre. Vous pouvez y indiquer un nom de fichier et un emplacement où l'enregistrer.

9.3.5 Personnalisation du Gestionnaire de files d’attente et de statistiques

9.3.5.1 Fichier MDstats.ini

Personnalisation du Gestionnaire de files d’attente et de statistiques

Liste des paramètres qui peuvent être modifiés dans le fichier `MDstats.ini` se trouvant dans le répertoire `\app\` de MDaemon:

[MDaemon]

AppDir=C:\mdaemon\app\	Emplacement du répertoire \app\ de MDaemon.

[QueueOptions]

Editor=NOTEPAD.EXE	Éditeur à utiliser lorsque l’on double-clique ou que l’on clique avec le bouton droit sur un message, et que Modifier est sélectionné.
LockOnEdit=No	Créer ou non un fichier LCK lors de la modification d’un message. Cela empêche à un message d’être sorti de la file d’attente lorsqu’il est en cours de modification.
AutoRefresh=Yes	Durée (en secondes) entre les actualisations automatiques de la liste de messages. 0 signifie :pas d’actualisation.
ShowDirectories=Yes	Montre les sous-répertoires des files d’attente dans la liste, en plus des messages. Les répertoires s’affichent sous la forme <NomRépertoire>.

[UserOptions]

ShowQuota=Yes	Détermine si la liste d’utilisateurs affiche ou non les informations de quota (compte de messages et espace disque selon l’estimation de MDaemon) ou les informations de fichiers (nombre de fichiers et espace disque total).

[LogOptions]

ShowUnknown=Yes	Affiche les sessions pour lesquelles MDStats n’a pas pu déterminer si elles sont entrantes ou sortantes, SMTP ou POP.
ShowSmtpInbound=Yes	Affiche les sessions SMTP entrantes.
ShowPopInbound=Yes	Affiche les sessions POP entrantes (vérifications du courrier).

ShowSmtpOutbound=Yes	Affiche les sessions SMTP sortantes.
ShowPopOutbound=Yes	Affiche les sessions POP sortantes (MultiPOP, DomainPOP).
ShowRFC822=Yes	Affiche les distributions de courrier local RFC822.
ShowSmtpHelo=Yes	Pour les sessions entrantes SMTP, affiche le domaine HELO dans la colonne Hôte.
IgnoreEmptyPop=Yes	Ignore les vérifications du courrier lorsqu' aucun message n'est distribué.
ShowImap=Yes	Affiche les sessions IMAP.
[Remap]	Remappe la lettre du lecteur, pour l'exécution de MDStats depuis un ordinateur différent que celui sur lequel se trouve MDaemon.
C:=\\server\c	Lors de la lecture depuis MDaemon.ini, remplace "C:" par "\\server\c".
[Special]	
OnlyOneInstance=No	Empêche l'exécution simultanée de plusieurs instances du Gestionnaire de files d'attente et de statistiques.

Voir également :

Paramètres du gestionnaire de files d'attente et de statistiques en ligne de commande 448

9.3.5.2 Paramètres en ligne de commande

Remarque : tous les paramètres de ligne de commandes ne sont pas sensibles à la casse.

Nombre de 1 à 8 — Affiche une file d'attente indiquée dans la Page files d'attente.

1 = File d'attente distante

2 = File d'attente locale

3 = File d'attente de relance

4 = File d’attente LAN

5 = File d’attente RAW

6 = File d’attente de messages erronés

7 = File d'attente entrante

8 = Enregistrer la file d’attente

/L[N] [InputFile] [OutputFile]	Produit un rapport de fichier journal. En indiquant un "N" après le "L", cela signifie : "ne pas enregistrer sous forme de fichier délimité par des virgules".
/A	Si un rapport de fichier journal est crée, ajoute de nouvelles informations dans le fichier plutôt que de l’écraser.



Section X

10 Fonctionnalités supplémentaires de MDaemon

10.1 Fichiers texte

MDaemon utilise de nombreux fichiers textes pour stocker des données, modèles de messages générés automatiquement ainsi que des paramètres, afin d'offrir un système aussi flexible que possible. Il est possible d'en créer de nouveaux en cliquant sur le menu Fichier » Nouveau. Cela permet de créer rapidement des fichiers de données pour les autorépondeurs ou diverses fonctionnalités de MDaemon, comme les fichiers RAW.

Modification des fichiers texte de MDaemon

Les fichiers de données de MDaemon sont au format texte et peuvent être modifiés dans le Bloc-notes. Il est possible d'y accéder en cliquant sur Fichier » Ouvrir » Nouveau fichier texte. La boîte de dialogue qui s'ouvre affiche par défaut les fichiers `.txt` du répertoire `\app\` de MDaemon.

10.2 Contrôle du serveur à distance par e-mail

De nombreuses fonctions de MDaemon sont accessibles à distance à l'aide du système de transport du courrier. Par exemple, vous pouvez accéder à divers paramètres de votre compte et les modifier en envoyant des messages formatés de façon spécifique au serveur. Vous pouvez également vous inscrire ou vous désinscrire de listes de diffusion, recevoir par e-mail des fichiers encodés... Pour cela, les messages envoyés au serveur doivent être adressés à "MDaemon@nomdudomaine.com".

Certaines de ces commandes requièrent un compte valide sur le serveur et son protégées par un mot de passe. Si un compte valide est exigé, le message doit être envoyé avec SMTP AUTH. Les commandes se saisissent dans le corps du message. Il est possible d'envoyer plusieurs commandes dans le même message, en indiquant une commande par ligne.

Il existe trois catégories de commandes pouvant être envoyés par e-mail : accès et modification du compte 452, contrôle des listes de diffusion et catalogues 454, et commandes générales 456.

Voir également :

Accès et modification du compte 452
Contrôle des listes de diffusion et catalogues 454
Commandes générales 456

10.2.1 Accès et modification du compte

L'utilisation des commandes suivantes requiert un compte de messagerie valide sur le serveur. De plus, le message doit avoir été envoyé avec SMTP AUTH. Les paramètres

indiqués entre crochets sont facultatifs. Par exemple, « nom [adresse] » peut être saisi simplement sous la forme « Lois » ou avec le paramètre (« Lois LLane@dailyplanet.com »). Pour en savoir plus sur l'utilisation de ces commandes par e-mail, voir : Contrôle du serveur à distance par e-mail 452.

COMMANDE	PARAMÈTRES SPÉCIAUX	DESCRIPTION
ACCOUNT INFO	aucun	L'état du compte mentionné dans l'objet est renvoyé par e-mail à l'expéditeur du message. Ex. : ACCOUNT INFO
PASSWORD	nouveau mot de passe	Le mot de passe du compte mentionné dans l'objet est remplacé par le mot de passe indiqué. Ex. : PASSWORD kryptonite
BEGIN SIGNATURE	aucun	Commence l'enregistrement d'un fichier de signatures à ajouter dans les messages envoyés par le compte mentionné dans l'objet. Les lignes suivantes sont considérées comme le texte de la signature.L'enregistrement s'arrête lorsque le mot END est rencontré. REMARQUE : le fichier de signature n'est disponible que pour les messages au format RAW. Le fichier de signature n'est pas ajouté aux messages RFC-2822 arrivant sur le serveur par SMTP ou POP. Dans ce cas la signature doit être ajoutée par le client de messagerie.
BEGIN AUTORESPONDER	aucun	Commence l'enregistrement d'un message d'autorépondeur pour le compte mentionné dans l'objet. Les lignes suivantes sont considérées comme le texte de l'autorépondeur. L'enregistrement s'arrête lorsque le mot END est rencontré. Exemple : BEGIN AUTORESPONDER Je suis actuellement en congés. Je vous répondrai dès que possible. END Pour effacer un autorépondeur activé, envoyez un message vide comme suit : BEGIN AUTORESPONDER END
FORWARD TO	adresse	L'adresse de transfert du compte mentionné dans l'objet est remplacée par celle indiquée, et

		elle est activée. Ex. : `FORWARD TO vacationing@myhost.com`
`UNFORWARD`	aucun	Le transfert de courrier est désactivé pour le compte mentionné dans l'objet. Ex. : `UNFORWARD`
`MULTIPOP`	on/off	La collecte MultiPOP est activée (ON) ou désactivée (OFF) pour le compte mentionné dans l'objet. Ex. : `MULTIPOP ON`

Voir également :

Contrôle du serveur à distance par e-mail 452
Contrôle des listes de diffusion et catalogues 454
Commandes générales 456

10.2.2 Contrôle des listes de diffusion et catalogues

Les commandes suivantes ne requièrent pas un compte sur le serveur. Les paramètres indiqués entre crochets sont facultatifs. Par exemple, « nom [adresse] » peut être saisi sous la forme « Clark » ou avec le paramètre optionnel « Clark CKent@dailyplanet.com ». Pour en savoir plus sur l'utilisation de ces commandes par e-mail, voir : Contrôle du serveur à distance par e-mail 452.

COMMANDE	PARAMÈTRES SPÉCIAUX	DESCRIPTION

`SUBSCRIBE`	nomdelaliste [adresse] [{nomréel}] [(motdepasse)]	L'expéditeur du message est inscrit automatiquement à la liste indiquée (à condition qu'elle supporte cette commande). Si vous indiquez une adresse après le nom de la liste, c'est cette adresse qui est ajoutée (et non celle de l'expéditeur). Il est possible d'ajouter le nom réel entre accolades.
		Si vous indiquez un mot de passe entre parenthèses, cette commande s'applique même si la liste est configurée pour l'ignorer.
		Exemple :
		`SUBSCRIBE mdsupp`
		`SUBSCRIBE mdsupp me@mydomain.com {Frank T}`
		`SUBSCRIBE mdsupp you@yourdom.com`

		(PASS)

UNSUBSCRIBE ou SIGNOFF	nomdelaliste [adresse] [(motdepasse)]	L'expéditeur du message est désinscrit de la liste indiquée (à condition qu'elle supporte cette commande). Si vous indiquez une adresse après le nom de la liste, c'est cette adresse qui est supprimée (et non celle de l'expéditeur).
		Si vous indiquez un mot de passe entre parenthèses, cette commande s'applique même si la liste est configurée pour l'ignorer.
		Exemples :
		`UNSUBSCRIBE MDSUPP (MDSPASS)`
		`SIGNOFF MDSupportList me@mydomain.com`

DIGEST	nomdelaliste [adresse]	Configure le compte indiqué en mode Compilation. Si aucune adresse n'est indiquée, la commande s'applique à l'expéditeur du message.
		Exemples :
		`SET DIGEST MDSupportList`
		`SET DIGEST mdsupp joe@mdaemon.com`

NORMAL	nomdelaliste [adresse]	Configure le compte indiqué en mode normal (et non compilation). Si aucune adresse n'est indiquée, la commande s'applique à l'expéditeur du message.
		Exemples :
		`NORMAL MDSupportList@mydomain.com`
		`NORMAL mdsupp@domain.com joe@altn.com`

NOMAIL	nomdelaliste [adresse]	Configure le compte indiqué en mode "nomail". Ce compte est alors suspendu et ne reçoit plus les messages de la liste. Si aucune adresse n'est indiquée, la commande s'applique à l'expéditeur du message. Exemple : `NOMAIL list@mydomain.com me@mydomain.com`

MAIL	nomdelaliste [adresse]	Rétablit le compte indiqué en mode normal (et non "nomail"). Si aucune adresse n'est indiquée, la commande s'applique à l'expéditeur du message.
		Exemples :
		`MAIL list@mydomain.com`
		`MAIL list@mydomain.com me@mydomain.com`

REALNAME	nomdelaliste [adresse] {nomréel}	Configure la valeur "Nom réel" pour l'adresse appartenant à la liste indiquée. Le nom réel doit être entre { }. Exemple : `REALNAME mdsupp@altn.com {Frank Thomas}`
GET	catalogue nom magique (motdepasse)	Récupère un fichier dans le catalogue indiqué, l'encode en MIME et l'envoie par e-mail à l'expéditeur du message ou à l'adresse indiquée dans une commande RESULTS TO. REMARQUE : le catalogue PUBLIC ne nécessite pas de nom ou de mot de passe. Exemple : `GET utils myutil (mypass)`
DIR	catalogue	Renvoie un répertoire des fichiers et mots de passe disponibles dans le catalogue. Exemple : `DIR public`

Voir également :

Contrôle du serveur à distance par e-mail 452
Accès et modification du compte 452
Commandes générales 456

10.2.3 Commandes générales

Commandes générales pouvant être envoyées au serveur par e-mail. Pour en savoir plus sur l'utilisation de ces commandes par e-mail, voir : Contrôle du serveur à distance par e-mail 452.

COMMANDE	PARAMÈTRES SPÉCIAUX	DESCRIPTION
HELP	aucun	Un copie du fichier NEWUSERHELP. DAT est envoyée par e-mail à l'expéditeur du message.
RESULTS TO	adresse	Le résultat des commandes suivantes est envoyé à l'adresse indiquée (et non à l'expéditeur du message).

		Exemple :
		
		`RESULTS TO someone@somewhere.com`
		`LIST MDSUPP`

`STATUS`	aucun	Un rapport indiquant les opérations effectuées et l'état du serveur est renvoyé à l'expéditeur du message. Ces données étant confidentielles, l'objet du message doit contenir le nom d'utilisateur et le mot de passe d'un compte administrateur.

Voir également :

[Contrôle du serveur à distance par e-mail](452) 452
[Accès et modification du compte](452) 452
[Contrôle des listes de diffusion et catalogues](454) 454

10.3 Les messages RAW

10.3.1 Les messages RAW

MDaemon prend en charge un format de message simple et puissant à la fois nommé courrier RAW. Le but du système RAW est de fournir un format standard simple que les systèmes logiciels tels que MDaemon peuvent utiliser pour créer des messages compatibles RFC-2822 beaucoup plus complexes. L'utilisation d'agents de transport de courrier comme RAW permet au logiciel client de confier au serveur tout le travail de conformité avec les standards de messagerie Internet.

Le courrier RAW consiste en une série d'en-têtes requis ou optionnels suivis d'un corps de message. La plupart des en-têtes sont composés d'une chaîne ("token") suivie d'une valeur entre <>. Chaque ligne d'en-tête se termine par une combinaison de caractères <CRLF>. Les en-têtes sont séparés du corps du message par une ligne vide et ne respectent pas la casse, et seuls les en-têtes "FROM" et "TO" sont requis. Tous les textes, en-têtes et corps sont en ASCII non crypté et doivent figurer dans un fichier dont l'extension est RAW (par exemple : "mon-message.raw").

Éviter le Filtre de contenu

Par défaut, les messages RAW sont soumis au Filtre de contenu comme s'il s'agissait de messages normaux. Si vous souhaitez qu'un message RAW spécifique ne soit pas soumis au Filtre de contenu renommez-le afin qu'il commence par « p » ou « P » (par exemple : « P_mon-message.raw »).



Les messages n'étant pas soumis au Filtre de contenu ne seront pas signés par DK ou DKIM. Si MDaemon est configuré de façon à signer tous les messages, cela risque de causer des problèmes de distribution. Pour que MDaemon signe les messages RAW n'étant pas soumis au Filtre de contenu, utilisez le paramètre x-flag=sign indiqué ci-dessous.

En-têtes RAW

From <mailbox@host.com>	Ce champ contient l'adresse électronique de l'expéditeur.
To <mailbox@host.com [, mailbox@host.com] >	Ce champ contient les adresses électronique des destinataires. Il est possible d'indiquer plusieurs destinataires en les séparant par des virgules.
ReplyTo <mailbox@host.com>	Adresse électronique à laquelle les réponses à ce message seront transmises (facultatif).
CC <maibox@host.com[, mailbox@host.com]>	Liste facultative de destinataires mis en copie de ce message. Il est possible d'indiquer plusieurs destinataires en les séparant par des virgules.
Subject <texte>	Objet du message (facultatif).
Header <En-tête: valeur>	Permet de placer explicitement des combinaisons en-tête/valeur dans le message et ainsi d'intégrer des en-têtes personnalisés ou non standard.

Champs spécifiques pris en charge par RAW

Pièces jointes et encodage

`x-flag=attach <filepath, method> [-x]`

Exemple : `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

Ce X-FLAG indique la valeur "ATTACH" ainsi que deux paramètres entre les caractères <>. Le premier caractère est un chemin complet vers le fichier à joindre à ce message. Le second paramètre qui est séparé du premier par une virgule, indique la méthode d'encodage à utiliser lorsque le message est joint. MDaemon supporte deux valeurs pour ce paramètre. La méthode MIME charge le serveur d'utiliser simplement la méthode Base64, standard d'Internet pour l'encodage de messages. La méthode ASCII charge le serveur d'importer seulement le fichier dans le message. Un paramètre supplémentaire X à la fin de la chaîne charge le serveur de retirer le fichier du disque une fois qu'il a été joint.

Notification de distribution

```
x-flag=confirm_delivery
```

Lors de la conversion d'un message RAW contenant ce marqueur dans un courrier RFC-2822, la chaîne est transformée en "Return-Receipt-To: <sender@host.org>".

Placer des combinaisons en-tête/valeur dans des messages RFC-2822

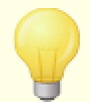
```
header <en-tête: valeur>
```

Si vous souhaitez placer une combinaison en-tête/Valeur dans les messages RFC-2822 qui seront générés par le fichier RAW, vous devrez utiliser la macro HEADER figurant dans la liste ci-dessus. Par exemple, si vous voulez que l'en-tête "Delivered-By: mail-machine@domain.com" soit placé dans le message RFC-2822, placez ceci : "header <Delivered-By: mail-machine@domain.com>" dans le message RAW. Sachez que la macro "header" requiert à la fois le champ et la valeur. Vous pouvez placer autant de macros "header" que vous le souhaitez dans un message RAW.

Signatures DK/DKIM des messages RAW

```
x-flag=sign
```

Lorsque cette commande est incluse dans un fichier *.raw, le message est signé par DK/DKIM. Ne l'utilisez que pour les messages RAW configurés pour éviter le Filtre de contenu (dont le nom commence par "p" ou "P"). N'ajoutez pas cette commande dans les messages RAW traités par le Filtre de contenu car ils sont signés normalement.



Tous les messages RAW générés par le Filtre de contenu utilisent automatiquement la commande x-flag=sign.

Exemples de messages RAW

Exemple 1 :

```
from <mdaemon@altn.com>
to <JohnSmith@somewhere.com>

Salut John!
```

Exemple 2 :

```
from <JohnSmith@nowhere.com>
to <President@Whitehouse.gov>
subject <Secret FBI Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\secret\files\dole.zip, MIME> -X

Voilà les fichiers que vous aviez demandés.
```

10.4 Fichiers sémaphore

MDaemon supporte les fichiers sémaphores qui peuvent être utilisés dans plusieurs buts. MDaemon recherche à intervalles réguliers dans le sous-répertoire \APP\ l'existence de ces fichiers. S'il en trouve un, le comportement associé est déclenché et le fichier sémaphore retiré. C'est un mécanisme simple qui permet aux administrateurs et/ou aux développeurs de manipuler MDaemon sans utiliser réellement l'interface. Voici une liste de tous les fichiers sémaphore et de leurs actions :

NOM DU FICHIER	ACTION
ADDUSER.SEM	Ce sémaphore crée de nouveaux comptes. Il sert à forcer MDaemon à ajouter de nouveaux enregistrements à la fin du fichier USERLIST.DAT sans provoquer une reconstruction complète de la base de données utilisateur qui pourrait prendre du temps. Chaque ligne de ce fichier doit correspondre à l'enregistrement complet de compte de la forme indiquée dans la section "Account Management Functions" de l'API de (voir `MD-API.html` dans le répertoire `\docs\API\`). Il est possible d'indiquer plusieurs nouveaux comptes à raison d'un enregistrement de compte par ligne. MDaemon traitera ce fichier ligne par ligne et ajoutera chaque nouveau compte. Vous pouvez créer ADDUSER.LCK pour verrouiller le fichier pendant que vous le mettez à jour et MDaemon ne touchera pas à ADDUSER.SEM avant que ADDUSER.LCK soit supprimé. Pour voir un exemple de fichier ADDUSER.SEM, ouvrez ADDUSER.SMP dans votre répertoire APP avec un éditeur de texte.
ALERT.SEM	Présente dans un pop-up le contenu du fichier sémaphore à tous les utilisateurs de WorldClient qui sont connectés lorsque le fichier est créé. Cependant, il ne s'affiche pas de suite sur tous les postes des utilisateurs, mais apparaît individuellement, au moment où le navigateur d'un utilisateur lance une requête vers le serveur WorldClient. **Remarque :** contrairement aux autres fichiers sémaphores, celui-ci est particulier à WorldClient. Ne l'enregistrez pas dans le répertoire \app\, mais dans le répertoire \MDaemon\WorldClient\.
ALIAS.SEM	Recharge le fichier contenant les alias.

AUTORESPEXCEPT.SEM	Recharge le(s) fichier(s) contenant les exceptions de l'autorépondeur.
BATV.SEM	Recharge le fichier de la protection contre les retours de courriers indésirables (BATV).
BAYESLEARN.SEM	Lance le processus d'apprentissage bayésien (comme si l'on cliquait sur le bouton Apprentissage de l'onglet Filtre bayésien du Filtre anti-spam). Remarque : ce fichier lance l'apprentissage bayésien même si cette fonctionnalité est désactivée.
BLACKLIST.SEM	Recharge le(s) fichier(s) de liste noire.
CATLIST.SEM	Recharge le cache contenant les noms des catalogues.
CFILTER.SEM	Recharge les règles et nettoie les données en cache du Filtre de contenu ; recharge la Liste blanche (pas de filtrage) 223.
CLEARQUOTACOUNTS.SEM	Les résultats des vérifications des quotas des utilisateurs sont conservés dans le fichier quotacounts. dat. Si vous souhaitez nettoyer ce cache pour un utilisateur, saisissez son adresse dans ce fichier SEM et placez-le dans le répertoire \app\. Si une ligne de ce fichier contient uniquement le caractère "*" le cache est nettoyé pour tous les comptes.
DELUSER.SEM	Vous pouvez utiliser ce fichier sémaphore pour supprimer un ou plusieurs comptes utilisateurs. Créez un fichier texte contenant les adresses de chaque compte que vous voulez supprimer (une adresse par ligne), nommez le fichier "DELUSER.SEM", puis déplacez le dans le répertoire \app\ de MDaemon. MDaemon supprimera les comptes, puis le fichier DELUSER.SEM.
DOMAINSHARING.SEM	Recharge le fichier de données du partage de domaines.
EDITUSER.SEM	Ce sémaphore sert à mettre à jour des enregistrements spécifiques dans le fichier USERLIST.DAT sans une reconstruction complète qui pourrait prendre du temps. Pour mettre à jour un enregistrement spécifique dans USERLIST.DAT, élaborez un enregistrement de remplacement complet selon le format indiqué dans la

section "Account Management Functions" de l'API MDaemon (voir MD-API.html dans le sous-répertoire de MDaemon \docs\API\). Ce nouvel enregistrement prendra en compte les modifications qui doivent être mises à jour dans USERLIST.DAT. Comme MDaemon reconnaît-il l'enregistrement à mettre à jour dans USERLIST.DAT? En ajoutant au début du nouvel enregistrement l'adresse électronique de l'enregistrement original suivie d'une virgule. Le fichier EDITUSER.SEM peut contenir plusieurs enregistrements à mettre à jour – chacun sur sa propre ligne. MDaemon traitera le fichier ligne par ligne. Vous pouvez créer EDITUSER.LCK pour verrouiller le fichier pendant que vous le mettez à jour et MDaemon ne touchera pas à EDITUSER.SEM avant que EDITUSER.LCK soit supprimé. Pour voir un exemple de fichier EDITUSER.SEM, ouvrez EDITUSER.SMP dans votre répertoire APP avec un éditeur de texte.

EXCPTION.SEM	Force MDaemon à recharger le fichier EXCPTION.DAT.
EXITNOW.SEM	Ferme MDaemon.
GATEWAYS.SEM	Afin d'optimiser les performances, MDaemon conserve la liste des passerelles en mémoire. Créez un fichier appelé GATEWAYS.SEM dans le répertoire APP de MDaemon pour recharger le fichier gateways.dat.
GREYLIST.SEM	Recharge le(s) fichier(s) de données de la liste grise.
GROUPS.SEM	Recharge le(s) fichier(s) de données des comptes.
GRPLIST.SEM	Recharge le cache contenant les noms des listes de diffusion.
HANGUPG.SEM	Provoque la fermeture d'une session RAS connectée. MDaemon attend que toutes les sessions de messagerie en cours se ferment et raccroche alors la session RAS.
HANGUPR.SEM	Force la fermeture d'une session RAS connectée. C'est un raccrochage immédiat et sans condition sans tenir compte des sessions de messagerie en cours sur la connexion.

HOSTSCREEN.SEM	Recharge le(s) fichier(s) de données de l'Écran d'hôte.
IPSCREEN.SEM	Recharge le(s) fichier(s) de données de l'Écran IP.
LDAPCACHE.SEM	Recharge le(s) fichier(s) de données des utilisateurs LDAP et utilisateurs de passerelles.
LOCKSEMS.SEM	Empêche le traitement de tous le fichiers sémaphore tant que ce fichier n'est pas supprimé.
LOGSETTINGS.SEM	Recharge les paramètres de journalisation.
MDSPAMD.SEM	Recharge la liste blanche du Filtre anti-spam et de MDSPAMD, ce qui l'oblige à réinitialiser toutes ses données de configuration.
MXCACHE.SEM	Recharge le(s) fichier(s) de données du cache MX.
NODNSBL.SEM	Recharge la liste blanche DNSBL.
ONLINE.SEM	MDaemon crée ce fichier sémaphore lors de l'établissement d'une connexion au FAI à l'aide de RAS. MD retire le sémaphore à la fin de la connexion. Cela est utile si vous voulez savoir quand MD utilise le sous-système RAS.
POSTDIAL.SEM	MDaemon crée ce fichier immédiatement après le décrochage d'une connexion effectuée par MDaemon.
PREDIAL.SEM	MDaemon crée ce fichier juste avant de tenter d'utiliser RAS/DUN. Cela permet aux autres logiciels de détecter lorsqu'il doit libérer le port de connexion pour que MDaemon puisse l'utiliser.
PRIORITY.SEM	Recharge le(s) fichier(s) de données du courrier prioritaire.
PROCBAD.SEM	Provoque le traitement de la file d'attente des messages erronés.
PROCDIG.SEM	Provoque l'envoi immédiat des compilations de listes de diffusion.

`PROCHOLDING.SEM`	Provoque le traitement de la file temporaire.
`PROCNOW.SEM`	Provoque la vérification du courrier distant et la distribution du courrier en file d'attente. **Remarque :** il est possible de générer automatiquement ce fichier en envoyant un e-mail à l'adresse "`procnow@mondomaine.com`". Par conséquent, "`procnow`" ne peut pas être utilisé comme nom de boîte aux lettres.
`PROCREM.SEM`	MDaemon passera immédiatement en mode traitement du courrier et traitera tout le courrier distant.
`PROCRETR.SEM`	Provoque le traitement de la file de relance.
`PRUNE.SEM`	Recharge les paramètres de nettoyage automatique.
`QUEUERUN.SEM`	Juste avant le début d'une session de messagerie, MDaemon crée ce fichier sémaphore. Il contient un horodatage indiquant la date et l'heure du dernier intervalle de traitement du courrier.
`RESTART.SEM`	Arrête et redémarre MDaemon.
`RESTARTCF.SEM`	Arrête et redémarre `CFEngine.exe` (l'exécutable du Filtre de contenu).
`RELOADCACHE.SEM`	Recharge tous les paramètres et les fichiers en cache à l'exception des paramètres et des fichiers du Filtre de contenu.
`REVERSEEXCEPT.SEM`	Recharge le fichier des exceptions de la vérification inverse.
`SCHEDULE.SEM`	Recharge le(s) fichier(s) de données de la programmation.
`SPAMHONEYPOTS.SEM`	Recharge le(s) fichier(s) de données des pièges à spam.
`SPF.SEM`	Recharge le(s) fichier(s) de données SPF, DK, DKIM et VBR.

`SUPPRESS.SEM`	Recharge les paramètres de liste noire et nettoie les paramètres des domaines en cache.
`TARPIT.SEM`	Recharge le(s) fichier(s) de données du système de répulsion et de l'Écran dynamique.
`TRANSLAT.SEM`	Recharge le(s) fichier(s) de données de la conversion d'en-têtes.
`TRAY.SEM`	Rétablit l'icône de MDaemon dans la zone de notification.
`TRUST.SEM`	Recharge la liste des domaines et adresses IP autorisés.
`UPDATEAV.SEM`	Lance la mise à jour des définitions de virus pour SecurityPlus for MDaemon.
`UPDATESA.SEM`	Lance la mise à jour du Filtre anti-spam.
`USERLIST.SEM`	Recharge le fichier `USERLIST.DAT`.
`WATCHDOG.SEM`	MDaemon recherche et retire ce sémaphore du répertoire APP approximativement toutes les 10 ou 20 secondes. Ce fichier peut être utilisé par des applications externes pour vérifier si MDaemon est en cours d'exécution. Si ce fichier reste dans le répertoire APP plus de 20 secondes, c'est signe que MDaemon n'est plus exécuté.

10.5 Système de priorité des messages

Cette fonctionnalité vous permet d'attribuer un ordre de priorité entre 0 et 99 aux messages. Cette valeur indique l'ordre de traitement des messages au cours de la distribution. Plus la valeur est basse, plus le message est important et plus il sera placé haut dans la file d'attente de messages. Ainsi, MDaemon tentera de distribuer un message avec une valeur de 10 avant un message avec une valeur de 90. Pour indication : 10 = Urgent, 50 = Normal et 80 = En masse.

Vous trouverez des options relatives à cette fonctionnalité dans l'onglet En-têtes164 des préférences et dans l'onglet Options379 de l'éditeur de liste de diffusion. Vous pouvez également utiliser l'action *Add extra header item to message*180 du Filtre de

contenu pour insérer l'en-tête Precedence dans les messages.

10.6 Re-routage

Généralement, un fichier de message en attente dans une file d'attente contient toutes les informations nécessaires pour que le message soit distribué à l'emplacement adéquat. Des en-têtes sont stockés dans le fichier .MSG (comme l'en-tête X-MDaemon-Deliver-To) et fournissent à MDaemon les instructions concernant le lieu et la personne à qui le message doit être distribué. Cependant, il est parfois utile ou nécessaire de passer outre ces informations et de fournir des alternatives au lieu et à la personne à qui un fichier .MSG doit être envoyé. Le re-routage fournit justement ce type de mécanisme. Un fichier de re-routage fournit à MDaemon des instructions très précises concernant le lieu et la personne à qui le fichier de message doit être envoyé. Si un fichier de re-routage existe pour un fichier de message particulier, les paramètres du premier– et non ceux du fichier .MSG– déterminent où et à qui le message est envoyé.

Les fichiers de re-routage se terminent par une extension .RTE. Par exemple, si un fichier de message en attente d'être envoyé se nomme MD0000.MSG ; le fichier de re-routage correspondant à ce message se nommera MD0000.RTE et doit se situer dans le même répertoire (file d'attente de courrier) que le fichier de message.

Le format d'un fichier de re-routage se présente comme suit :

```
[RemoteHost]
DeliverTo=remote-domain.com
```

Cette section d'un ficher de re-routage indique à MDaemon le serveur auquel doit être envoyé le fichier .MSG correspondant. MDaemon tentera toujours une connexion directe à l'hôte qui essaye d'acheminer le message aussi rapidement que possible. Il n'est possible d'indiquer qu'un hôte.

```
[Port]
Port=xxx
```

Ce paramètre indique le port sur lequel la connexion TCP/IP et la tentative de distribution doivent se faire. 25 est le port par défaut pour le courrier SMTP.

```
[LocalRcpts]
Rcpt0=adresse@mon-domaine.com
Rcpt1=autre-adresse@mon-domaine.com
Rcpt2=encore-une-autre-adresse@mon-domaine.com

[RemoteRcpts]
Rcpt0=adresse@domaine-distant.com
Rcpt1=autre-adresse@domaine-distant.com
Rcpt2=encore-une-autre-adresse@domaine-distant.com
```

Ces sections du ficher de re-routage vous permettent d'indiquer un nombre illimité de destinataires locaux et distants qui recevront une copie du fichier .MSG associé. Les adresses de destinataires locaux et distants doivent être séparées et placées dans les

sections [LocalRcpts] et [RemoteRcpts] correspondantes.

Les fichiers de re-routage fournissent un mécanisme permettant de distribuer ou de rediriger des messages, mais ne sont pas toujours nécessaires. MDaemon utilise les fichiers de re-routage pour le courrier "routé" de liste de diffusion. Lorsqu'une liste de diffusion est configurée pour acheminer une seule copie d'un message de la liste à un hôte distant, un fichier de re-routage est alors utilisé. C'est une méthode particulièrement efficace de distribution lorsque vous devez distribuer du courrier à des adresses en masse, puisqu'une seule copie du message est nécessaire alors que vous pouvez indiquer un nombre illimité de destinataires. Néanmoins, tous les hôtes distants ne permettent pas ce type d'acheminement. Comme c'est eux qui en définitive doivent distribuer une copie du fichier de message à chaque adresse, certains hôtes placent une limite maximale de destinataires que vous pouvez indiquer.

10.7 MDaemon et les serveurs proxy

MDaemon est conçu pour être particulièrement souple d'emploi. Par conséquent, il peut être configuré pour de nombreuses configurations réseau et de nombreux produits. Sa flexibilité lui permet de fonctionner correctement avec des serveurs proxy LAN. Pour configurer MDaemon afin qu'il fonctionne sur n'importe quel proxy, assurez-vous simplement que les paramètres des ports 41 que vous utilisez ne provoquent pas de conflits avec les paramètres que vous avez définis pour le serveur proxy. Par exemple, le courrier SMTP se fait normalement sur le port 25. Comme une adresse IP ne peut disposer que d'un seul port 25, deux serveurs ne peuvent écouter le courrier SMTP au même moment et sur le même ordinateur. Lorsque vous essayez d'intégrer MDaemon avec un proxy, nous vous recommandons, dès que cela est possible, de donner à MDaemon le contrôle sur le traitement et la distribution du courrier. Pour cela, les ports SMTP, POP, IMAP et autres dans le proxy doivent être désactivés pour que MDaemon puisse effectuer la distribution du courrier de façon indépendante.

Toutefois, si vous jugez qu'il est nécessaire d'acheminer le courrier à travers un proxy, MDaemon vous permet de configurer les ports qu'il utilisera pour envoyer et recevoir les transactions SMTP/POP/IMAP. Vous pouvez avoir besoin d'attribuer à ces ports des valeurs non standard afin de filtrer vos transactions SMTP/POP/IMAP à travers un serveur proxy ou un pare-feu.

Pour en savoir plus sur la configuration de MDaemon avec un serveur proxy, veuillez consulter les ressources disponibles sur le site : www.altn.com.



Section XI

11 Glossaire

ACL (Access Control Lists)—ACL est une extension du protocole IMAP4 (Internet Message Access Protocol) qui permet de créer une liste d'accès pour vos dossiers IMAP. Ainsi, les utilisateurs qui possèdent un compte sur votre serveur de messagerie peuvent accéder à vos dossiers. Divers niveaux d'autorisation sont possibles : vous pouvez par exemple indiquer si un utilisateur est autorisé ou non à supprimer des messages, à les marquer comme lus ou non lus, à copier des messages vers des dossiers, à créer des sous-dossiers, etc. Seuls les clients de messagerie compatibles avec ACL peuvent être utilisés pour partager cet accès et définir des autorisations. Toutefois, si votre client de messagerie n'est pas compatible avec ACL, vous pouvez définir des autorisations depuis l'interface graphique de MDaemon. Peu de clients de messagerie prennent directement en charge ACL mais il existe un utilitaire nommé InsightConnector (disponible sur le site www.bynari.net) capable d'ajouter cette fonctionnalité (et bien d'autres encore) à Microsoft Outlook.

Pour en savoir plus sur le protocole ACL, consultez le document RFC 2086 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2086.txt

Adresse de courrier électronique—Nom ou chaîne de caractères identifiant une boîte aux lettres électronique spécifique sur un réseau et à laquelle est envoyé du courrier électronique. Les adresses de courrier électronique sont les points de départ et d'arrivée des messages. Les serveurs de messagerie ont besoin de ces adresses pour pouvoir distribuer les messages. La forme des adresses diffère selon le type de réseau mais sur Internet, toutes les adresses de courrier électronique se construisent de la façon suivante : "boiteauxlettres@domaine.com"

Exemple :

Frank.Thomas@altn.com

Adresse IP—Parfois appelée "numéro IP", l'adresse IP sert à identifier un réseau TCP/IP particulier ainsi que les hôtes ou les ordinateurs sur ce réseau. Il s'agit d'une adresse numérique de 32 octets contenant quatre nombres entre 0 et 255 séparés par des points (par exemple. "127.0.0.1"). Dans un réseau isolé, chaque ordinateur doit disposer d'une adresse IP unique qui peut être assignée aléatoirement. Cependant, chaque ordinateur sur Internet doit disposer d'une adresse IP enregistrée afin d'éviter des doublons. Chaque adresse IP peut être soit dynamique, soit fixe. Les adresses IP fixes ne varient pas et représentent toujours le même emplacement ou ordinateur sur Internet. Les adresses IP dynamiques changent et sont généralement assignées par un FAI aux ordinateurs qui se connectent temporairement à Internet (accès commuté). Une adresse IP fixe peut néanmoins être attribuée à un compte à accès commuté. Les FAI et les grandes entreprises tentent généralement d'acquérir un ensemble ou une plage d'adresses IP auprès du service d'enregistrement InterNIC afin que tous les clients sur leur réseau ou utilisant leur service disposent d'adresses similaires. Cet ensemble se divise en trois classes : A, B, et C. Les ensembles des classes A et B sont utilisés par les très grandes entreprises et prennent respectivement en charge 16 millions d'hôtes et 65.000 hôtes. Les ensembles de la classe C servent aux réseaux plus petits et

prennent en charge 255 hôtes. Les ensembles des classes A et B sont à présent difficiles à obtenir en raison du manque d'adresses disponibles. Par conséquent, la plupart des entreprises doivent se contenter de plusieurs ensembles de classe C. Ce manque d'adresses IP a débouché sur la création d'un nouveau protocole IP, Classless Inter-domain Routing (CIDR), destiné à remplacer progressivement l'ancien système. Pour en savoir plus sur le protocole IPv4, consultez le document RFC-791 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc791.txt

Pour en savoir plus sur IPv6, consultez le document RFC-2460 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2460.txt

Pour en savoir plus sur CIDR, consultez les documents RFC 1517 à 1519 aux adresses suivantes :

http://www.rfc-editor.org/rfc/rfc1517.txt
http://www.rfc-editor.org/rfc/rfc1518.txt
http://www.rfc-editor.org/rfc/rfc1519.txt

À la volée—La locution "à la volée" possède deux sens. Tout d'abord, elle désigne une chose pouvant être faite "rapidement" ou facilement "parmi" d'autres tâches à effectuer. Par exemple, un logiciel de comptabilité peut prendre en charge la création de comptes "à la volée" tout en saisissant des chiffres concernant les ventes (Cessez de saisir des chiffres, cliquez sur le bouton X, saisissez un nom, puis continuez à saisir des chiffres). Ensuite, la locution "à la volée" s'emploie pour désigner quelque chose qui se génère dynamiquement (ou automatiquement) et non de façon manuelle ou statique. Par exemple, en utilisant les informations stockées dans un "témoin de connexion", une page Web personnalisée peut se générer "à la volée" lorsqu'un utilisateur se rend à nouveau sur un site. Au lieu de demander la création d'une page personnalisée en fonction des tâches de l'utilisateur, elle sera générée dynamiquement en fonction des actions de la personne.

Analyser—En informatique, "analyser" (parse) signifie diviser un langage informatique en parties qui peuvent être utiles à l'ordinateur. Un analyseur dans un compilateur prend chaque avertissement de programme écrit par un développeur et le divise en parties qui peuvent être utilisées pour développer d'autres actions ou pour créer les instructions formant un programme exécutable. Le serveur MDaemon analyse souvent les messages électroniques afin de déterminer leur destination ou de les traiter à l'aide de filtres et d'autres outils

ASCII—Se prononce "aski". ASCII est l'acronyme de "American Standard Code for Information Interchange". C'est un code standard composé de 7 bits qui remplace les lettres latines majuscules, minuscules et la ponctuation par un nombre compris entre 0 et 127 (0000000 à 1111111). Par exemple, le code ASCII pour le M majuscule est 77. La plupart des ordinateurs remplacent le texte par des codes ASCII pour transférer des données vers d'autres ordinateurs. Les éditeurs de texte et les traitements de texte sont généralement capables de stocker des fichiers au format ASCII (parfois appelés fichiers ASCII). Toutefois, la majorité des fichiers de données, en particulier ceux qui contiennent des données numériques, n'est pas stockée au format ASCII.Certains ensembles de caractères plus volumineux disposent de 128 caractères supplémentaires car ils utilisent 8 bits au lieu de 7. Ces

caractères supplémentaires représentent des symboles et des caractères non anglais. Le système d'exploitation DOS utilise un ensemble supplémentaire d'ASCII appelé ASCII étendu ou high ASCII. ISO Latin 1 est un standard quasi universel utilisé par la plupart des systèmes d'exploitation et des navigateurs Web.

ATRN—Voir ETRN ou ODMR.

Bande passante—Total des données mesuré en bits par seconde (bps) pouvant être transmis en un laps de temps donné à travers un réseau ou une connexion par modem. Une page pleine de texte anglais correspond à environ 16.000 bits et se transfère en 1 ou 2 secondes avec un modem rapide. Une vidéo en plein écran nécessite approximativement 10.000.000 bits par seconde, en fonction de la compression. Comparons la bande passante à une autoroute : l'autoroute représente la connexion, les voitures qui roulent dessus les données de l'ordinateur. Plus l'autoroute est large (plus la bande passante est grande), plus un grand nombre de voitures peuvent rouler dessus.

Baud—Unité servant à mesurer la fréquence à laquelle les signaux changent de valeur sur une ligne téléphonique. C'est une référence à la vitesse de transmission de données d'un modem. Pour les modems les plus lents, on parle de "taux de bauds" alors que pour les modems haut débit, on parle de "bits par seconde". "Taux de baud" et "bits par seconde" ne sont pas nécessairement synonymes puisque chaque signal peut encoder plus d'un bit dans des connexions à haut débit.

Bit (Binary digit)—Il s'agit de la plus petite unité d'information stockée dans un ordinateur, ayant la valeur 1 ou 0 et appartenant au système de numérotation binaire. Son abréviation correspond à un "b" minuscule comme dans "bps" (bits par seconde). Une page de texte fait en général 16 000 bits.

Bitmap—Un "bitmap" est une carte de points (ou bits) formant une image tant que vous ne fermez pas l'écran ou que vous n'agrandissez pas trop la carte. Les fichiers bitmap les plus courants sont BMP, JPEG, GIF, PICT, PCX et TIFF. Comme les images bitmap sont composées de groupes de points, les zooms donnent des résultats peu satisfaisants (blocs). Les graphiques vecteurs (habituellement créés avec CorelDraw, PostScript ou des logiciels de création assistée par ordinateur) s'agrandissent mieux car il s'agit de formes géométriques générées mathématiquement et non de points.

Boîte aux lettres—Zone en mémoire ou sur un dispositif de stockage appartenant à une adresse électronique spécifique et dans laquelle sont stockés les messages électroniques. Dans tous les systèmes de messagerie électronique, chaque utilisateur dispose d'une boîte aux lettres privée dans laquelle sont stockés les messages lorsque le serveur de messagerie de cet utilisateur les reçoit. Le terme "boîte aux lettres" est souvent utilisé pour faire référence à la partie la plus à gauche dans une adresse électronique. Par exemple, "Frank" dans "Frank@altn.com" est la boîte aux lettres, tandis que "altn.com" est le nom de domaine.

Bps (bits par seconde)—Mesure la vitesse de déplacement des données d'un endroit à un autre. Par exemple, un modem 33.6 kbps peut transférer 33.600 bits par seconde. Kilobit (1000 bits) par seconde et mégabit (100 000 bits) par seconde sont respectivement abrégés par "Kbps" et"Mbps".

Cache—Sert à enregistrer les informations récemment utilisées pour qu'elles soient

rapidement accessibles la fois suivante. Par exemple, un navigateur Web utilise un cache pour y enregistrer des pages, des images, des URL et d'autres éléments issus de sites que vous avez récemment visités. Lorsque vous consultez à nouveau une page enregistrée dans le cache, le navigateur n'a plus besoin de télécharger ces éléments. La vitesse de navigation est largement supérieure puisque l'accès au cache sur votre disque dur est plus rapide que l'accès à Internet. Le cache IP de MDaemon enregistre les adresses IP des domaines auxquels vous avez dernièrement envoyé des messages. Ainsi, MDaemon n'a pas à revérifier ces adresses lorsqu'il envoie d'autres messages aux mêmes domaines. Cette fonctionnalité accélère la distribution des courriers électroniques.

Carte d'accès distant—Sous Windows, élément qui permet de connecter votre ordinateur à un réseau via un modem. Si votre ordinateur n'est pas connecté à un réseau local (LAN) muni d'un accès à Internet, vous devez configurer la carte d'accès distant pour qu'elle se connecte au point de présence (POP) puis à votre fournisseur d'accès (FAI) avant d'accéder à Internet. Votre FAI devra transmettre des informations telles que l'adresse de la passerelle et l'adresse IP de votre ordinateur. La carte d'accès distant est disponible à partir de l'icône Poste de travail. Il est possible de configurer un profil de connexion différent pour chaque service en ligne utilisé. Une fois la configuration terminée, vous pouvez copier le raccourci de chaque profil sur le Bureau pour pouvoir établir une connexion en double-cliquant sur l'icône.

Carte réseau—Composant d'un circuit informatique qui permet à un ordinateur d'être connecté à un réseau. Les cartes réseau offrent une connexion réseau ininterrompue alors qu'un modem (utilisé par la plupart des ordinateurs de particuliers pour se connecter à un réseau par le biais de lignes téléphoniques) ne proposent généralement qu'une connexion temporaire. La plupart des cartes réseau sont conçues pour des types de réseaux et de protocoles spécifiques (cf. Ethernet et TCP/IP).

CIDR (Classless Inter-Domain Routing)—Système d'adressage IP remplaçant l'ancien système basé sur les classes A, B et C. Les adresses IP CIDR se composent d'une adresse IP normale suivie d'une barre oblique et d'un nombre formant le "préfixe IP".

Exemple :

123.123.0.0/12

Le préfixe IP détermine le nombre d'adresses gérées par le système d'adressage CIDR. Les nombres les plus petits sont ceux qui englobent le plus d'adresses. Dans l'exemple ci-dessus, le préfixe IP "/12" peut être utilisé pour 4096 adresses de l'ancienne classe C. Les adresses CIDR réduisent la taille des tables de routage et permettent d'obtenir plus d'adresses IP. Pour en savoir plus sur le système CIDR, consultez les documents RFC 1517 à 1519 aux adresses suivantes :

http://www.rfc-editor.org/rfc/rfc1517.txt
http://www.rfc-editor.org/rfc/rfc1518.txt
http://www.rfc-editor.org/rfc/rfc1519.txt

CGI (Common Gateway Interface)—Ensemble de règles décrivant comment un serveur Web communique avec un autre élément logiciel sur une même machine et

comment cet autre élément (le programme CGI) communique avec le serveur Web. Chaque élément de logiciel peut être un programme CGI s'il gère l'entrée et la sortie des documents conformément à la norme CGI. Les programmes CGI extraient des données d'un serveur Web et les traitent (ex. : insertion du contenu d'un formulaire dans un courrier électronique). Ils s'enregistrent dans le répertoire "cgi-bin" d'un site Web et apparaissent dans l'URL qui permet de les atteindre.

cgi-bin—Nom servant à désigner le répertoire dans lequel sont enregistrés les programmes CGI sur un serveur Web. L'élément "bin" dans "cgi-bin" est la contraction de "binary" car la plupart des programmes de référence sont "binaires". Dans la pratique, les programmes cgi-bin sont des fichiers texte, des scripts exécutés par des programmes externes.

Client—Logiciel qui permet de contacter un programme serveur, de lui envoyer des données ou, au contraire, d'en recevoir. Le serveur est généralement installé sur un autre ordinateur, soit sur le réseau local, soit ailleurs. Chaque programme client est conçu pour fonctionner avec un ou plusieurs programmes serveur et vice versa. Les navigateurs Web sont l'exemple de clients capables de communiquer avec des serveurs Web.

Client de messagerie (ou client)—Application logicielle qui permet d'envoyer, de recevoir et d'organiser du courrier électronique. On l'appelle client car les systèmes de messagerie sont basés sur une architecture client-serveur : le client sert à rédiger un courrier électronique, à l'envoyer au serveur qui l'achemine ensuite vers le serveur du destinataire sur lequel il sera retiré par le client du destinataire. En général, les clients de messagerie sont des applications logicielles indépendantes installées sur l'ordinateur de l'utilisateur. Néanmoins, le serveur WorldClient de Alt-N Technologies contient un client intégré qui s'affiche dans le navigateur web de l'utilisateur. Cette caractéristique permet d'éviter une installation supplémentaire et d'améliorer le transfert du courrier électronique.

Commutation de paquets—Traitement de l'envoi et de la réception de paquets sur un réseau ou sur Internet. Par opposition à la commutation de circuits (cf. téléphone analogique) qui envoie des données dans un flux continu sur un seul chemin ou circuit, la commutation de paquets transmet les données divisées en "paquets" qui ne prennent pas obligatoirement le même chemin pour parvenir à destination. De plus, comme les données sont dans des unités séparées, plusieurs utilisateurs peuvent envoyer simultanément différents fichiers sur le même chemin.

Courrier électronique— encore appelé "e-mail". Le courrier électronique correspond à la transmission de messages texte sur des réseaux de communication. La plupart des réseaux informatiques disposent d'un système de messagerie électronique. Certains systèmes dépendent d'un seul réseau tandis que d'autres disposent de passerelles vers d'autres réseaux (qui leur permettent de communiquer depuis plusieurs emplacements) ou vers Internet (ce qui leur permet d'envoyer du courrier dans le monde entier). La plupart des systèmes de messagerie incluent un client de messagerie (comporte un éditeur de texte et d'autres outils pour la rédaction des messages) et un ou plusieurs serveurs (reçoivent le courrier envoyé par les clients puis l'acheminent vers la destination appropriée). Les messages sont rédigés à l'aide du client puis transférés au serveur qui les envoie à l'adresse électronique indiquée dans le message. Enfin, ils sont acheminés par le serveur vers un autre serveur qui stocke le courrier destiné à cette adresse. Si la destination du message correspond à une adresse locale dont le serveur d'origine est responsable, le courrier peut être

stocké sur ce serveur plutôt que d'être acheminé vers un autre. Enfin, le destinataire du message se connectera au serveur et retirera son courrier à l'aide de son client de messagerie. Le transfert de messages électroniques depuis votre client vers le serveur de destination ne prend que quelques secondes ou minutes. Les messages électroniques peuvent également inclure des pièces jointes. Il peut s'agir de n'importe quel type de fichier : fichiers texte, fichiers programme, autres messages électroniques, etc. Toutefois, comme la plupart des systèmes de messagerie électronique n'acceptent que l'envoi de fichiers texte, les pièces jointes doivent d'abord être codées (converties en format texte) avant de pouvoir être envoyées, puis décodées lorsqu'elles parviennent à destination. Ce processus se fait généralement automatiquement par les clients de messagerie expéditeurs et récepteurs. Tous les Fournisseurs d'Accès à Internet (FAI) proposent des services de messagerie. La plupart d'entre eux prennent en charge les passerelles pour que vous puissiez échanger du courrier avec des utilisateurs d'autres systèmes de messagerie. Même s'il existe plusieurs protocoles pour le traitement du courrier électronique, plusieurs standards communs permettent aux utilisateurs d'échanger des messages sur pratiquement tous les systèmes.

Courrier indésirable (également appelé "spam")—Courrier électronique non sollicité à vocation publicitaire envoyé par des "spammeurs" (ils parviennent à recueillir des milliers, voire des centaines de milliers d'adresses électroniques à partir de plusieurs sources). Le spam est devenu un sérieux problème sur Internet. Il est synonyme de gaspillage de temps et de ressources du serveur. Comme les "spammeurs" utilisent plusieurs techniques pour masquer l'origine du message (usurpation d'adresses pour se faire passer pour quelqu'un d'autre ou tentative de relais du spam via plusieurs serveurs de messagerie), il est particulièrement difficile de l'éviter. Le serveur MDaemon est doté d'un certain nombre de fonctionnalités spécialement conçues pour lutter contre le spam : système de blocage de spam, bouclier IP, Écran IP, commande de renvoi, etc. L'origine du mot " spam " vient d'une marque anglaise de corned-beef : Spice Pork And Meat (pâté épicé à base de porc et de viandes). Le mot SPAM a ensuite été repris dans un sketch des célèbres Monty Python, où dans un café, une serveuse et des vikings chantent à tue-tête le mot SPAM, afin d'inciter un client à en consommer.

Cryptage—Mesure de sécurité. Le cryptage consiste à coder les informations contenues dans un fichier afin qu'elles ne soient intelligibles qu'une fois décodées ou décryptées. Le cryptage est fréquemment utilisé dans le courrier électronique pour qu'une tierce personne ne puisse pas lire cecourrier si elle l'intercepte. Le message est crypté lorsqu'il est envoyé, puis décrypté à son arrivée.

DHCP (Dynamic Host Control Protocol)—Protocole utilisé par les serveurs d'un réseau pour l'attribution dynamique d'adresses IP aux ordinateurs du réseau. Un serveur DHCP attend qu'un ordinateur se connecte à lui avant de lui assigner une adresse IP depuis une liste stockée. Pour en savoir plus sur le protocole DHCP, consultez le document RFC -2131 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2131.txt

DomainPOP—Développé par Alt-N Technologies et partie intégrante du serveur MDaemon, DomainPOP permet d'offrir un service de messagerie à un réseau local ou à un groupe de travail à partir d'une seule boîte aux lettres POP chez un FAI. Avant, si le serveur de messagerie d'une entreprise ne disposait pas d'une connexion Internet "en direct" et permanente, chaque personne devait disposer de sa propre

boîte aux lettres chez le FAI de l'entreprise pour pouvoir bénéficier d'un service de messagerie. Avec DomainPOP, une seule boîte aux lettres est nécessaire. Le FAI sonde tous les messages régulièrement collectés par DomainPOP pour le nom de domaine de l'entreprise dans cette boîte aux lettres. Ensuite, DomainPOP analyse les messages pour déterminer les destinataires visés et distribue le courrier dans les boîtes aux lettres des utilisateurs locaux. Le réseau entier dispose ainsi d'un service de messagerie électronique à partir d'un seul compte chez un FAI.

Ethernet—Type de connexion le plus courant utilisé dans un réseau local. Les deux formes les plus utilisées d'Ethernet sont 10BaseT et 100BaseT. Un Ethernet 10BaseT peut transférer des données à des vitesses de 10 mbps (mégabits par seconde) par connexion câble ou sans fil. Un Ethernet 100BaseT transfère des données à des vitesses de 100 mbps. Un Ethernet Gigabit transfère des données à un taux maximal de 1000 mbps (utilisé par certains ordinateurs Apple).

ETRN (Extended TURN)—Extension du protocole SMTP qui permet l'envoi d'une requête d'un serveur SMTP à un autre pour envoyer ou retirer du courrier d'une file d'attente. Le protocole SMTP n'étant pas prévu pour les demandes de courrier (requêtes exécutées par les protocoles POP ou IMAP), cela permet au serveur SMTP d'effectuer une requête ETRN pour que le serveur distant démarre une session SMTP et commence l'envoi du courrier stocké vers l'hôte indiqué dans la requête. La commande TURN n'était pas fiable en termes de sécurité : la session SMTP inversait la direction et commençait à envoyer le courrier stocké sans avoir vérifié l'authenticité du serveur. La commande ETRN démarre une nouvelle session SMTP plutôt que d'inverser la direction. Par conséquent, si le serveur qui lance la requête usurpe l'identité d'un hôte, le serveur d'envoi essaiera de distribuer le courrier à l'hôte réel. Il existe un autre standard doté de la commande ATRN (Authenticated TURN) qui, comme TURN, inverse la direction de la session SMTP mais requiert une authentification. Ce standard s'appelle ODMR (On-Demand Mail Relay). Les commandes ETRN et ATRN (standard ODMR) sont prises en charge par le serveur MDaemon. Pour en savoir plus sur ETRN, consultez le document RFC 1985 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc1985.txt

Pour en savoir plus sur ODMR, consultez le document RFC 2645 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2645.txt

Fabricant de matériel informatique d'origine (OEM)—Ce terme est souvent confus et mal interprété. Un fabricant d'équipement est une entreprise qui utilise l'équipement ou les produits d'une autre entreprise dans son propre produit qui est emballé et vendu sous une marque ou le nom d'une entreprise différents. Par exemple, HyperMegaGlobalCom, Inc. est un fabricant d'équipement car il achète des composants informatiques à une ou plusieurs entreprises, les assemble en un seul produit personnalisé, puis le vend sous la marque "HyperMegaGlobalCom". L'entreprise qui a vendu à HyperMegaGlobalCom les composants peut également être un fabricant d'équipement si elle se fournit en composants auprès d'une autre entreprise à son tour. Le terme "Fabricant d'équipement" est malheureusement impropre car les fabricants d'équipement sont les "envelopperus" ou "personnaliseurs". En dépit de cela, les gens utilisent toujours régulièrement le terme "Fabricant d'équipement" lorsqu'ils se réfèrent aux véritables fabricants de matériel

informatique au lieu de ceux qui les ré-enveloppent—d'une façon compréhensible.

FAI (Fournisseur d'Accès à Internet)—Entreprise qui fournit un accès et des services Internet à un utilisateur final. La plupart des FAI offrent plusieurs services Internet à leurs clients : accès Web, messagerie électronique, accès à des groupes de discussion et à de nouveaux serveurs, etc. En général, les utilisateurs se connectent au FAI à l'aide d'une connexion téléphonique (ou autre), le FAI les connecte au routeur qui, à son tour, les dirige sur Internet.

FAQ—"Foire Aux Questions". Les FAQ sont des documents qui répondent aux questions les plus fréquemment posées sur un sujet donné. Elles se présentent sous forme de liste, chaque question étant suivie d'une réponse. Dans les FAQ de grande taille, les questions sont répertoriées au début du document et comportent des renvois (ou des liens hypertextes) à la question et à la réponse dans le document. Les FAQ sont d'une aide précieuse, elles vous font gagner du temps et vous évitent de contacter le support technique.

FTP (File Transfer Protocol)—Méthode simple et efficace de transfert de fichiers d'un ordinateur à un autre via Internet. Il existe des applications client/serveur spécifiques conçues dans ce but et appelées "serveurs FTP" et "clients FTP" (FTP Voyager et CuteFTP sont les deux clients les plus courants). En général, les clients FTP peuvent remplir d'autres fonctions en plus du transfert de fichiers (ce sont des produits particulièrement utiles). Certains navigateurs web sont compatibles avec le protocole FTP même s'ils ne gèrent souvent que le téléchargement. Pour les navigateurs compatibles avec le protocole FTP, il suffit de se connecter au site FTP en saisissant "ftp://…" dans l'URL au lieu de "http://…".

Pour en savoir plus sur le protocole FTP, consultez le document RFC-959 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc959.txt

GIF (Graphics Interchange Format)—GIF utilise des couleurs indexées ou une palette comprenant un certain nombre de couleurs. La taille des fichiers est ainsi réduite, en particulier lorsque l'image contient de grandes zones de la même couleur, et leur transfert plus rapide.

Hôte—Tout ordinateur sur un réseau qui agit comme un serveur pour d'autres ordinateurs sur le même réseau. L'ordinateur hôte peut exécuter un serveur Web, un serveur de messagerie ou d'autres services (il fournit généralement plusieurs services à la fois). Sur les réseaux poste-à-poste, les ordinateurs sont souvent hôte et client en même temps. Par exemple, un ordinateur héberge l'imprimante réseau mais il sert également de client pour collecter le courrier et télécharger des fichiers depuis un autre hôte.

HTML (Hypertext Markup Language)—Langage servant à créer des documents hypertexte utilisés sur le Web. Un document HTML est un document en texte simple qui contient des codes de mise en forme et des balises que le navigateur web de l'utilisateur interprète et exécute dans la page qu'il affiche. Par exemple, si le navigateur reçoit un document HTML qui contient "<B>Texte</B>", le mot "Texte" apparaît en gras. Comme les fichiers en texte simple sont de très petite taille, ils se transfèrent rapidement sur Internet.

HTTP (Hypertext Transfer Protocol)—Protocole de transfert des fichiers hypertexte sur Internet. Le protocole HTTP requiert un programme client (généralement un navigateur Web) et un serveur HTTP. Pour en savoir plus sur le protocole HTTP, consultez le document RFC-2616 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2616.txt

Hypertexte—Tout texte contenant un hyperlien ou un renvoi vers un autre document/un autre endroit dans un même document. On parle également de "lien hypertexte" ou simplement de "lien". L'hypertexte est un mot ou une phrase dans lequel/laquelle on insère un lien qui, en cliquant dessus, ouvre un autre document ou vous guide vers un autre emplacement mis en signet. En général, les liens hypertextes se distinguent par leur soulignement et leur couleur différente, mais ce n'est pas toujours le cas. Parfois, l'hypertexte est semblable au texte normal et seule la modification graphique de votre curseur en pointant dessus vous indique qu'il s'agit d'un lien.

Identifiant—Code ou série de caractères unique permettant d'accéder ou de s'identifier sur un serveur ou un ordinateur. Dans la plupart des cas, un mot de passe doit accompagner cet identifiant pour obtenir l'accès. Il existe de nombreux synonymes, comme nom d'utilisateur, ID utilisateur, etc.

IMAP—Développé par l'Université de Stanford, le protocole IMAP (Internet Message Access Protocol) sert à gérer et à retirer des messages électroniques. La dernière version, IMAP4, est identique à POP3 mais elle dispose de fonctionnalités supplémentaires. IMAP4 permet de gérer le courrier électronique sur le serveur plutôt que sur l'ordinateur local de l'utilisateur (il est possible de rechercher des mots clés dans les messages, ces messages peuvent être organisés dans des dossiers, être sélectionnés pour être téléchargés, etc. tout en étant toujours sur le serveur). Ainsi, le protocole IMAP désencombre l'ordinateur de l'utilisateur et centralise le courrier pour plus de possibilités d'accès.

Pour en savoir plus sur le protocole IMAP, consultez le document RFC -2060 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2060.txt

Interface Utilisateur Graphique (GUI)—L'interface utilisateur graphique permet, grâce à un dispositif de pointage, de cliquer sur des éléments graphiques affichés à l'écran plutôt que de taper du texte dans une ligne de commande. Les systèmes d'exploitation Microsoft Windows et Apple Mac fonctionnent avec une interface utilisateur graphique. Même si cette idée d'interface a été premièrement présentée par Apple, elle provient en fait de Xerox.

Internet—Créé en 1969 par l'armée américaine, son but premier était de servir de réseau de communication indestructible même en cas de guerre nucléaire. Il représente aujourd'hui des millions d'ordinateurs et de réseaux de par le monde. Internet n'est pas centralisé—il n'est pas contrôlé par une entreprise, une organisation ni un pays. Chaque hôte (ou machine) sur Internet est indépendant des autres et peut fournir toutes les informations ou services que ses opérateurs souhaitent rendre disponibles. Néanmoins, la plupart des informations transférées sur Internet passent par des "épines dorsales", des connexions haut débit à large bande passante contrôlées par les plus grands fournisseurs d'accès à Internet. La plupart

des utilisateurs accèdent à Internet via des services en ligne tels que AOL ou via des fournisseurs d'accès à Internet (FAI) qui sont connectés à l'une de ces épines dorsales. Nombreux sont ceux qui confondent le Web (World Wide Web) et Internet. Le Web ne représente qu'une partie d'Internet (partie majoritairement commerciale, la plus visible et la plus connue).

Intranet—Réseau de type Internet, de plus petite taille ou privé, souvent le réseau d'une entreprise ou d'un organisme. Bien que les intranets varient beaucoup d'une organisation à l'autre, ils peuvent contenir toutes les fonctionnalités disponibles sur Internet. Ils disposent souvent de leurs propres systèmes de messagerie, de répertoires de fichiers, de pages Web sur lesquelles naviguer, d'articles à lire, etc. La principale différence entre un intranet et Internet : en plus d'être petit, le réseau intranet est restreint à une organisation ou à un groupe.

Java—Développé par Sun Microsystems, Java est un langage de programmation informatique orienté réseau avec une syntaxe proche de C/C++ et une construction autour de classes (non de fonctions). Dans les applications Internet, il sert généralement à programmer des applets, petits programmes inclus dans les pages web. Ces programmes peuvent se télécharger automatiquement et s'exécuter via le navigateur de l'utilisateur. Ils offrent beaucoup de fonctions non disponibles avec HTML ou d'autres langages de script, le tout sans crainte de virus ou de dommages pour votre ordinateur. Comme Java est à la fois efficace et simple d'utilisation, il est de plus en plus utilisé par les concepteurs de logiciels et de matériel informatique.

JavaScript (à ne pas confondre avec Java)—Développé par Netscape, JavaScript est un langage de script conçu pour étendre les capacités du HTML et créer des pages Web interactives. Ce langage de programmation condensé et simple d'utilisation (plus simple que Java ou d'autres langages) est parfois limité. Il est néanmoins utile pour ajouter des éléments interactifs dans des sites web. Parexemple, il est idéal si vous souhaitez que des données soient traitées avant d'être soumises au serveur, ou que vos pages répondent à l'interaction de l'utilisateur avec des liens ou des éléments. Il peut servir à commander des modules d'extension, des applets et à utiliser de nombreuses autres fonctions. JavaScript est inclus dans le texte des documents HTML et s'exécute à l'aide des navigateurs Web.

JPEG—Format de fichier d'images plus efficace pour compresser des photographies en couleur que le format GIF. Alors que GIF est le meilleur choix pour les images aux formes régulières et aux couleurs répétées, JPEG convient davantage aux images présentant des motifs irréguliers et un grand nombre de couleurs. JPEG est le format le plus courant pour les photographies très colorées sur Internet. L'acronyme de JPEG signifie "Joint Photographic Experts Group", du nom du groupe qui a créé ce format.

Kbps—Généralement associé aux vitesses de modem (par exemple 56 Kbps), cet acronyme signifie "Kilobits Par Seconde". Il s'agit du nombre de kilobits (1000 bits) de données déplacées ou traitées chaque seconde. Notez qu'il s'agit de kilobits et non de kilooctets—un kilooctet contient huit fois plus de données qu'un kilobit.

Kilooctet—Un kilooctet (Ko) correspond à 1000 octets de données informatiques. Techniquement, il s'agit de 1024 octets (2^10 = 1024) mais pour plus de simplicité, on parle généralement de 1000 octets.

Latence—Temps que prend un ensemble de données pour traverser une connexion

réseau. Lors de l’envoi de données, il existe un temps “latent” durant lequel l’ordinateur expéditeur attend une confirmation de réception des données. La latence, en plus de la bande passante, est l’un des facteurs déterminant la vitesse de connexion.

LDAP (Lightweight Directory Access Protocol)—Protocole de gestion d’annuaires en ligne destiné à simplifier le protocole DAP (Directory Access Protocol). Le système d’annuaires est une structure hiérarchisée : ses divers niveaux sont la "racine" ou annuaire de départ, le pays, l’entreprise, le service de l’entreprise et l’individu de ce service. Chaque entrée LDAP comporte un ensemble d’attributs et un identificateur unique appelé DN (distinguished name). Comme il s’agit d’un protocole ouvert, efficace et adaptable à plusieurs serveurs, le protocole LDAP permet à presque toutes les organisations ou plates-formes d’accéder aux informations de l’annuaire pour trouver des adresses de courrier électronique, des entreprises ou des fichiers sur le Web.

Pour en savoir plus sur le protocole LDAP, consultez le document RFC -2251 à l’adresse suivante :

http://www.rfc-editor.org/rfc/rfc2251.txt

Liste de diffusion—(on parle parfois de "groupe de messagerie"). Liste d’adresses de courrier électronique identifiée par une seule adresse électronique (exemple : nomdelaliste@exemple.com). Lorsqu’un serveur de liste reçoit un message destiné à l’une de ses listes de diffusion, ce message est automatiquement distribué à tous les membres de la liste. Le serveur MDaemon est doté d’une suite complète de fonctionnalités qui permettent d’obtenir des listes publiques ou privées (n’importe qui peut poster ou s’abonner/seuls les membres peuvent poster ou s’abonner), modérées (chaque message doit être approuvé avant d’être acheminé sur la liste), envoyées en format compilation ou en messages individuels, etc.

Mégaoctet—Même s’il correspond, d’un point de vue technique, à 1.048.576 octets (ou 1024 kilooctets), le mégaoctet est généralement arrondi à un million d’octets. L’abréviation de mégaoctet est "Mo" (exemple : "20 Mo").

MIME (Multipurpose Internet Mail Extensions)—Définie en 1992 par IETF (Internet Engineering Task Force), cette méthode d’encodage standard est utilisée pour joindre des fichiers non texte dans des messages standards. En général, seuls les fichiers en texte clair peuvent être transférés par courrier électronique. Les fichiers non texte sont d’abord codés en format texte clair puis décodés lorsqu’ils arrivent à destination. Ainsi, un programme de messagerie est dit compatible MIME s’il peut à la fois recevoir et envoyer des fichiers à l’aide du standard MIME. Lors de l’envoi d’une pièce jointe codée MIME, le type de fichier envoyé et la méthode utilisée pour lui restituer sa forme initiale sont indiqués dans le message. Il existe de nombreux types de contenus MIME prédéfinis, comme "image/jpeg" et "text/plain". Il est toutefois possible de définir vos propres types de MIME. Le standard MIME est également utilisé par les serveurs Web pour identifier les fichiers qu’ils envoient aux navigateurs Web. Comme les navigateurs acceptent plusieurs types de codages MIME, ils peuvent afficher des fichiers qui ne sont pas en format HTML. De plus, en mettant à jour les listes de ces différents codages et le logiciel utilisé pour les traiter, de nouveaux formats de fichier sont rapidement acceptés.

Pour en savoir plus sur MIME, consultez les documents RFC 2045 à 2049 aux

adresses suivantes :

http://www.rfc-editor.org/rfc/rfc2045.txt
http://www.rfc-editor.org/rfc/rfc2046.txt
http://www.rfc-editor.org/rfc/rfc2047.txt
http://www.rfc-editor.org/rfc/rfc2048.txt
http://www.rfc-editor.org/rfc/rfc2049.txt

Miroir—Serveur (généralement un serveur FTP) qui dispose d'une copie des fichiers qui se trouvent sur un autre serveur. Son but est d'offrir un emplacement alternatif à partir duquel les fichiers dupliqués peuvent être téléchargés, si le serveur d'origine est défaillant ou surchargé.

Modem (contraction de modulateur-démodulateur)—Dispositif connecté à un ordinateur permettant le transfert de données vers d'autres ordinateurs par le biais de lignes téléphoniques. Le modem convertit les données numériques de l'ordinateur dans un format analogique (modulation) puis les transmet à un autre modem qui inverse le traitement (démodulation). Un modem est un convertisseur analogique-numérique et numérique-analogique. La vitesse de transfert des données est exprimée soit en bauds (exemple : 9600 bauds), soit en kilobits par seconde (exemple : 28,8 kbps).

MultiPOP—Composant du serveur de messagerie MDaemon pouvant collecter du courrier à l'aide du protocole POP3 simultanément depuis plusieurs serveurs de messagerie pour les utilisateurs MDaemon. MultiPOP est idéal pour les utilisateurs MDaemon qui disposent d'un compte de messagerie sur un autre serveur : leur courrier est collecté puis transféré sur leur compte. MultiPOP permet de stocker les messages de l'ensemble des utilisateurs dans une seule boîte aux lettres.

Navigateur—Application qui sert à afficher des pages Web et qui interprète le code HTML, le texte, les liens hypertexte, les images, le JavaScript, etc. Les navigateurs les plus utilisés sont Internet Explorer et Mozilla Firefox.

Nom de domaine—Il s'agit du nom unique qui identifie un site Web. Par exemple, "altn.com" est le nom de domaine de Alt-N Technologies. Chaque nom de domaine contient au moins deux parties séparées par des points, la plus à gauche est la plus spécifique, alors que la partie de droite est la plus générale. Chaque nom de domaine indique l'adresse IP d'un seul serveur, mais un seul serveur peut disposer de plusieurs noms de domaine. Par exemple, "mail.altn.com", "alt-n.com" et "somedomain.com" peuvent se référer au même serveur que "altn.com", mais "altn.com" ne peut se référer à deux serveurs différents. Il existe toutefois des méthodes permettant d'indiquer des serveurs alternatifs vers lesquels les clients seront dirigés si le serveur principal est défaillant ou indisponible. Souvent, le nom de domaine est enregistré mais il n'est pas connecté à un ordinateur réel : soit le propriétaire du nom de domaine n'a pas encore créé de site web, soit il dispose d'adresses électroniques sans site Web à maintenir. Dans ce dernier cas, un ordinateur Internet doit traiter le courrier du nom de domaine répertorié. Enfin, le terme "domaine" remplace souvent l'expression "nom de domaine". Le mot "domaine" a d'autres significations et désigne parfois un domaine Windows NT ou une classe de valeurs.

Pour en savoir plus sur les noms de domaines, consultez les documents RFC 1034 et 1035 aux adresses suivantes :

http://www.rfc-editor.org/rfc/rfc1034.txt
http://www.rfc-editor.org/rfc/rfc1035.txt

NNTP (Network News Transfer Protocol)—Protocole utilisé pour transférer et distribuer des messages sur des groupes de discussion USENET. Les clients de messagerie et les navigateurs les plus courants disposent désormais de clients NNTP intégrés. Pour en savoir plus sur le protocole NNTP, consultez le document RFC-977 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc977.txt

Noeud—Tout ordinateur connecté à un réseau.

Numéro IP—Voir Adresse IP au début du glossaire.

Octet—Ensemble de bits (généralement huit) représentant un seul caractère. Un octet comporte huit bits, parfois plus, tout dépend du type de mesure appliqué. "Octet" s'abrège par un "O" majuscule.

ODMR (On-Demand Mail Relay)—Protocole conçu pour permettre aux serveurs de messagerie non équipés d'une connexion permanente à un FAI ni d'une adresse IP fixe de recevoir du courrier tout comme les serveurs dotés d'une IP fixe et de la commande ETRN. Lorsqu'un système dispose d'une IP fixe, la commande ESMTP ETRN peut être utilisée. En revanche, pour les systèmes fondés sur des adresses IP dynamiques, il n'existe pas de solution. ODMR résout ce problème : il introduit la commande Authenticated TURN (ATRN) qui permet d'inverser le flux d'une session SMTP (comme l'ancienne commande TURN) et de demander une authentification du serveur pour plus de sécurité. Un serveur SMTP muni d'une adresse IP dynamique peut alors se connecter au FAI et le courrier d'un ou de plusieurs hôtes peut lui être distribué via le protocole SMTP (au lieu d'être collecté avec POP ou IMAP). Cette solution peu coûteuse répond à la demande des entreprises qui ont besoin de leur propre serveur de messagerie mais qui ne peuvent s'offrir une adresse IP fixe ou une présence en ligne.

Pour en savoir plus sur ODMR, consultez le document RFC 2645 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2645.txt

Paquet—Unité de données informatiques envoyée sur un réseau. Chaque fois que vous recevez des données d'un autre ordinateur sur votre réseau local ou sur Internet, elles arrivent dans votre ordinateur sous forme de "paquets". Le fichier ou le message d'origine est divisé en paquets, lesquels sont transmis puis rassemblés à leur arrivée. Chaque paquet contient un en-tête incluant sa source, sa destination, un bloc de données et un code de vérification d'erreur. Il est également "numéroté" afin de pouvoir être connecté aux paquets envoyés. Le traitement de l'envoi et de la réception de paquets est appelé "commutation de paquets". Les paquets sont couramment appelés "datagrammes".

Paramètre—Un paramètre est une caractéristique ou une valeur. En langage informatique, il s'agit de toute valeur transmise à un programme par un utilisateur ou un autre programme. Votre nom, votre mot de passe, un paramètre de préférence, une taille de police, etc. sont des paramètres. En programmation, un paramètre est

une valeur attribuée à une sous-routine ou une fonction à traiter.

Paramètres par défaut—Les paramètres par défaut correspondent aux valeurs prédéfinies des options dans les programmes informatiques. Il s'agit des valeurs appliquées lorsqu'aucun paramètre précis n'a été configuré par l'utilisateur. Les paramètres par défaut correspondent aux valeurs majoritairement choisies par les utilisateurs.

Pare-feu—Le pare-feu joue un rôle important en termes sécurité (tant au niveau des logiciels que des matériels). Il permet de diviser un réseau informatique en deux ou plusieurs sous-réseaux, ou d'en limiter l'accès à certains utilisateurs. Par exemple, vous pouvez autoriser vos utilisateurs à visualiser la page d'accueil d'un site Web hébergé sur votre réseau et leur y consacrer un espace privé. Peu importe la méthode employée (mot de passe exigé, accès autorisé à certaines IP seulement, etc.), cet espace "employés" est placé derrière un pare-feu.

Passerelle—Matériel informatique ou logiciel qui convertit des données entre deux applications ou réseaux avec des protocoles différents. "Passerelle" renvoie également aux moyens qui permettent d'accéder d'un système à un autre. Par exemple, votre FAI est une passerelle vers Internet. La fonctionnalité de passerelle de domaine du serveur de messagerie MDaemon lui permet d'agir en tant que passerelle de messagerie pour d'autres domaines : MDaemon collecte le courrier d'un domaine et le conserve jusqu'à ce que ce dernier le récupère. Cette fonctionnalité est très utile pour les domaines qui n'utilisent pas de connexion permanente à Internet et pour ceux qui ont besoin d'un serveur de sauvegarde en cas de défaillance du leur.

PDF (Portable Document Format)—Format multiplate-forme hautement compressé développé par Adobe Systems Incorporated et qui préserve la mise en forme du texte et des images du document pour de nombreuses applications. Le document peut ainsi s'afficher dans sa forme réelle et être imprimé avec précision sur plusieurs types de plates-formes (contrairement à de nombreux traitements de texte). Pour lire un fichier PDF, il faut utiliser Adobe Acrobat Reader, application gratuite distribuée par Adobe Systems. Il existe également un module d'extension pour visionner des fichiers PDF dans votre navigateur Web, ce qui évite de les télécharger et de les visualiser dans un autre programme.

Pièce jointe—Fichier joint à un courrier électronique. La plupart des systèmes de messagerie n'acceptent que l'envoi de fichiers texte. Par conséquent, si la pièce jointe est un fichier binaire ou un fichier texte mis en forme (fichier Word), il doit être codé avant d'être envoyé puis décodé une fois reçu. Il existe plusieurs techniques de codage dont deux principales : le protocole MIME (Multipurpose Internet Mail Extensions) et le codage Unix-to-Unix (Uuencode). Pour les messages entrants, le serveur de messagerie MDaemon peut confier le décodage des pièces jointes au client de messagerie du destinataire ou les décoder automatiquement puis les enregistrer à un emplacement précis avant de distribuer le message à l'utilisateur local.

Pilote—Petit programme qui communique avec certains matériels informatiques. Les pilotes contiennent des informations nécessaires à l'ordinateur et à d'autres programmes pour commander et reconnaître les matériels. Les ordinateurs Windows disposent généralement de pilotes sous forme de fichier DLL (dynamic link library). La plupart des matériels informatiques utilisés sur Mac n'ont pas besoin de pilotes, mais

lorsqu'un pilote est nécessaire, il s'agit généralement d'une extension de système.

Ping (Packet Internet Groper)—Programme Internet de base utilisé pour déterminer si une adresse IP précise est joignable et accepte des requêtes. Il procède de la sorte en envoyant une requête Echo ICMP (Internet Control Message Protocol) et en attendant une réponse. Pour en savoir plus sur les protocoles ICMP et Echo, consultez les documents RFC 792 et 862 aux adresses suivantes :

http://www.rfc-editor.org/rfc/rfc792.txt
http://www.rfc-editor.org/rfc/rfc862.txt

POP (Post Office Protocol)—POP (ou POP3) est le protocole de messagerie le plus utilisé pour le retrait de courrier depuis un serveur de messagerie. La plupart des clients de messagerie utilisent le protocole POP bien que certains utilisent également le protocole IMAP. POP2 est devenu un standard au milieu des années 80 et nécessitait SMTP pour l'envoi de messages. Il a été remplacé par la nouvelle version POP3 qui peut être utilisée avec ou sans SMTP.

Pour en savoir plus sur POP3, consultez le document RFC-1939 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc1939.txt

Port—Dans les réseaux TCP/IP, UDP et sur Internet, un port est le terminus d'une connexion logique identifié par un chiffre compris entre 0 et 65536. Les ports 0 à 1024 servent à utiliser certains protocoles et services. Par exemple, les serveurs Web sont généralement sur le port 80, les serveurs SMTP communiquent sur le port 25, et les serveurs POP envoient et reçoivent du courrier sur le port 25. Sur chaque ordinateur, un port donné est utilisé ou lié à un seul programme. En naviguant sur Internet, certains serveurs sont exécutés sur des ports différents de ceux configurés par défaut, ce qui vous oblige à indiquer le port dans l'URL en le précédant par deux-points. Exemple : www.exemple.com:3000. Le terme "port" est également utilisé en référence aux interfaces de connexion utilisées pour connecter des périphériques et du matériel informatique. Par exemple, les ports série, les ports USB, les ports parallèles, etc. Enfin, le terme "port" s'emploie pour décrire la conception d'un programme destiné à une plateforme spécifique ou à la fonction d'un ordinateur sur une autre plate-forme. Par exemple, "créer un port UNIX pour une application."

PPP (Point to Point Protocol)—Standard Internet pour les connexions par ligne téléphonique. PPP est un ensemble de règles chargé de définir l'échange de paquets de données entre votre ordinateur et d'autres systèmes sur Internet. Pour en savoir plus sur le protocole PPP, consultez le document RFC-1661 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocole—En langage informatique, un protocole est un ensemble de conseils et de standards par lesquels les serveurs et les applications communiquent. Il existe de nombreux protocoles utilisés dans différents buts. Par exemple, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, etc.

IP (Internet Protocol)—Le protocole IP permet le transfert de données entre des systèmes sur Internet. Sans tenir compte de la plate-forme de l'ordinateur ou du système d'exploitation, chaque ordinateur utilisant le même protocole Internet peut

transférer des données. Le terme "IP" est aussi généralement utilisé comme abréviation d' "adresse IP". Le protocole IP standard actuel est IP version 4 (IPv4).

Pour en savoir plus sur le protocole IP, consultez le document RFC-791 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc791.txt

Registre—Base de données utilisée par Microsoft Windows pour stocker des informations de configuration à propos des logiciels installés sur l'ordinateur. Y figurent les paramètres utilisateur, les associations d'extension de fichiers, l'arrière-plan du bureau, les couleurs et bien d'autres paramètres. Le Registre comprend les six parties suivantes :

HKEY_User—Stocke les informations utilisateur pour chaque utilisateur du système.
HKEY_Current_User—Préférences de l'utilisateur actuel.
HKEY_Current_Configuration—Stocke les paramètres de l'affichage et des imprimantes.
HKEY_Classes_Root—Associations de fichiers et informations OLE.
HKEY_Local_Machine—Matériel, système d'exploitation et paramètres des applications installées.
HKEY_Dyn_Data—Données de performances.

Lorsque vous installez des programmes, le fichier d'installation écrit automatiquement des informations dans le registre. Vous pouvez les modifier manuellement à l'aide du programme regedit.exe intégré à Windows. Soyez particulièrement vigilent car si vous modifiez le mauvais paramètre, votre ordinateur risque de ne plus fonctionner correctement, ou de ne plus fonctionner du tout.

Réseau—Deux ordinateurs ou plus reliés entre eux. L'objectif du réseau est de pouvoir partager ressources et informations entre plusieurs systèmes. Exemple : plusieurs ordinateurs peuvent partager la même imprimante, les mêmes lecteurs DVD-ROM, les mêmes disques durs, les mêmes fichiers individuels, etc. Il existe plusieurs types de réseaux, les plus courants étant les réseaux locaux (LAN) et les réseaux étendus (WAN). Dans un réseau local, les ordinateurs individuels (ou noeuds) sont géographiquement proches (souvent dans le même bâtiment). Ils sont directement reliés par câble, même si les connexions sans fil s'imposent peu à peu. Les noeuds d'un réseau étendu sont assez éloignés (dans un autre bâtiment ou une autre ville). Ils se connectent entre eux par ligne téléphonique ou par liaison satellite. Internet est un réseau. Il est souvent décrit comme un "réseau de réseaux".

Réseau étendu (Wide Area Network, WAN)—Réseau similaire à un LAN (Local Area Network) mais généralement étendu à plusieurs bâtiments, voire plusieurs villes. Les réseaux étendus sont parfois composés de réseaux locaux interconnectés. On pourrait dire qu'Internet est le plus grand réseau étendu du monde.

Réseau local (LAN)—Réseau limité à un seul bâtiment ou à une seule zone, composé de noeuds (ordinateurs ou postes de travail) reliés entre eux par des fils, des câbles ou par tout autre moyen. La plupart des grandes entreprises disposent d'un LAN, ce qui simplifie considérablement la gestion et le partage des informations pour les employés et les services. La plupart des réseaux locaux utilisent des systèmes de messagerie, de chat, de partage du matériel (cf. les imprimantes) pour

éviter d'avoir du matériel distinct pour chaque poste. Lorsque les noeuds du réseau se connectent par ligne téléphonique, ondes radios ou liens satellites, on parle de "réseau étendu" (WAN) et non plus de réseau local (LAN).

RFC (Request For Comments)—Document accompagnant la création d'un standard sur Internet. Chaque nouveau standard/protocole est publié sur Internet sous forme de "RFC". L'IETF (Internet Engineering Task Force) les utilise pour ouvrir des discussions sur les nouveaux standards avant de les valider. Une fois validés, même si aucun autre commentaire n'est requis, les standards sont toujours exposés dans les documents RFC et conservent leur numéro d'identification. Par exemple, la RFC 822 (à présent remplacée par la RFC 2822) est le document officiel concernant les courriers électroniques. Néanmoins, les protocoles officiellement adoptés comme "standards" sont également répertoriés sous un numéro officiel dans le document "Internet Official Protocol Standards" (lui même STD-1 et RFC-3000). Les documents RFC sont disponibles sur de nombreux sites Internet. La source officielle reste RFC Editor : http://www.rfc-editor.org/. Le document Internet Official Protocol Standards est situé à l'adresse suivante :

http://www.rfc-editor.org/rfc/std/std1.txt

RTF (Rich Text Format)—Format de fichier universel développé par Microsoft et compatible avec presque tous les traitements de texte. Par opposition au format de texte clair, RTF vous permet de conserver la mise en forme (police, couleur du texte, etc.). La taille des fichiers RTF peut être supérieure à celle d'autres formats de fichier, notamment les documents Word 2000 (*.doc) ou les PDF d'Adobe.

Serveur—Ordinateur ou programme offrant un service précis à un logiciel client installé sur d'autres ordinateurs. Le terme "serveur" renvoie à une partie d'un logiciel, comme un serveur SMTP, ou à un ordinateur sur lequel le logiciel est exécuté. Un seul ordinateur serveur peut exécuter plusieurs programmes serveur différents simultanément. Par exemple, le serveur du réseau peut exécuter un serveur Web, un serveur de messagerie, un serveur FTP, un serveur fax et d'autres serveurs à la fois.

Serveur de liste—Application serveur distribuant du courrier à plusieurs destinataires en envoyant le message à une seule adresse. Lorsqu'un message est adressé à une liste de diffusion maintenue par le serveur de liste, il est automatiquement retransmis aux membres de cette liste. En général, les listes de diffusion disposent d'une seule adresse électronique (par exemple, nomdelaliste@exemple.com) qui correspond en fait à une liste de destinataires et non à une personne ni à une boite aux lettres en particulier. Lorsque quelqu'un s'inscrit à une liste de diffusion, le serveur de liste ajoute automatiquement cette adresse à la liste et lui distribue les messages de la liste. Lorsque quelqu'un se désabonne, le serveur de liste supprime simplement son adresse afin qu'il ne reçoive plus les messages de la liste. Le terme "listserv" est souvent utilisé pour faire référence à un serveur de liste de diffusion. Toutefois, Listserv® est une marque déposée de L-Soft international, Inc., un programme spécifique développé par Eric Thomas pour BITNET en 1986. Outre ses nombreuses fonctionnalités, le serveur MDaemon est doté d'une suite complète de serveurs de liste ou de liste de diffusion.

SMTP (Simple Mail Transfer Protocol)—Protocole utilisé pour l'envoi de courrier sur Internet d'un serveur à un autre ou d'un client à un serveur. SMTP comporte un ensemble de règles relatives à l'interaction entre les programmes expéditeur et récepteur du courrier. Le courrier reçu par un serveur via le protocole SMTP est

souvent stocké sur ce serveur puis collecté par un client à l'aide du protocole POP, IMAP ou d'un autre protocole.

Pour en savoir plus sur le protocole SMTP, consultez le document RFC -2821 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc2821.txt

TCP/IP (Transmission Control Protocol/Internet Protocol)—Protocole au fondement d'Internet, TCP/IP englobe les protocoles de communication utilisés sur Internet pour se connecter à des hôtes. Il s'agit du protocole le plus utilisé sur les réseaux locaux. TCP/IP est un système à deux couches : la couche supérieure, TCP, gère la scission et l'assemblage des fichiers en paquets pour leur transmission sur le réseau ; la couche inférieure, IP, traite l'adressage des paquets afin qu'ils parviennent à destination. Pour en savoir plus sur TCP et IP, consultez les documents RFC 793 et 791 aux adresses suivantes :

TCP – http://www.rfc-editor.org/rfc/rfc793.txt
IP – http://www.rfc-editor.org/rfc/rfc791.txt

Téléchargement—Processus par lequel un ordinateur récupère ou obtient des données depuis un autre ordinateur. Par exemple, il est possible d'obtenir des informations sur Internet en les téléchargeant depuis d'autres ordinateurs. L'opération inverse (envoi de données vers un autre ordinateur) s'appelle "upload".

Telnet—Commande et programme utilisés pour se connecter à des sites Internet qui prennent en charge l'accès Telnet. La commande Telnet permet de s'identifier sur le serveur Telnet. Si vous possédez un compte sur ce serveur, vous pouvez accéder aux ressources autorisées (fichiers, courrier, etc.). L'inconvénient de Telnet est qu'il s'agit d'un programme de ligne de commande qui utilise les commandes Unix.

Pour en savoir plus sur Telnet, consultez les documents RFC 854 et 855 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc854.txt
http://www.rfc-editor.org/rfc/rfc855.txt

Terminal—Support permettant d'envoyer des commandes à un ordinateur distant. Un terminal est constitué d'un clavier, d'un écran et de quelques circuits. Les ordinateurs personnels sont parfois utilisés pour simuler des terminaux.

TIFF (Tagged Image File Format)—Format de fichier graphique considéré comme un standard de l'échange de fichiers entre plates-formes informatiques. TIFF peut traiter des niveaux de couleurs de 1 à 24 bits.

Traduction d'adresses réseau (NAT)—Système dans lequel deux ensembles d'adresses IP sont utilisés par un seul réseau (l'un pour le trafic externe, l'autre pour le trafic interne). Utilisé comme un pare-feu, ce système contribue à sécuriser le réseau. L'adresse IP de votre ordinateur visualisée par les postes extérieurs au LAN est différente de l'adresse IP réelle en local. Les matériels ou les logiciels placés "entre" votre réseau et Internet convertissent les adresses. Grâce à cette méthode, plusieurs postes d'un réseau local peuvent "partager" une adresse IP de l'entreprise. Personne ne peut connaître votre véritable adresse en dehors du réseau ni même se

connecter à votre ordinateur sans authentification pendant la traduction.

UDP (User Datagram Protocol)—UDP est l'un des protocoles inclus dans le protocole TCP/IP servant au transfert des données. UDP est souvent qualifié de protocole sans état car il ne confirme pas la réception des paquets envoyés. Pour en savoir plus sur UDP, consultez le document RFC -768 à l'adresse suivante :

http://www.rfc-editor.org/rfc/rfc768.txt

Unix (ou UNIX)—Système d'exploitation créé par Bell Labs dans les années 60. Conçu pour accueillir de nombreux utilisateurs, c'est le système d'exploitation le plus courant des serveurs sur Internet. Il existe plusieurs systèmes d'exploitation basés sur UNIX : Linux, GNU, Ultrix, XENIX, etc.

URL—Chaque fichier ou serveur sur Internet dispose d'une URL (Uniform Resource Locator). Il s'agit de l'adresse que vous saisissez dans votre navigateur Web pour accéder à un serveur ou à un fichier. Les URL ne peuvent pas contenir d'espaces et utilisent toujours des barres obliques. Elles sont composées de deux parties séparées par "://". La première partie est le protocole utilisé ou la ressource recherchée (par exemple, http, telnet, ftp, etc.) et la seconde est l'adresse Internet du fichier ou du serveur (par exemple, www.altn.com or 127.0.0.1).

Uuencode—Ensemble d'algorithmes permettant de convertir des fichiers dans des séries de caractères ASCII de 7 bits pour les transmettre sur Internet. Bien qu'il signifie Unix-to-Unix encode, il n'est plus réservé à UNIX. C'est devenu un protocole universel utilisé pour transférer des fichiers entre différentes plates-formes. C'est une méthode d'encodage fréquemment utilisée dans les courriers électroniques.

Zip—Se réfère à un fichier compressé ou "zippé", généralement avec l'extension de fichier ".zip". La compression d'un ou de plusieurs fichiers dans un seul fichier d'archive réduit l'espace de stockage et accélère la vitesse de transfert vers d'autres ordinateurs. Pour utiliser un fichier compressé, vous devez le décompresser avec un programme tel que PKZIP ou WinZip. De nombreux utilitaires de compression/décompression sont disponibles sur Internet.

Index

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -